ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Π.Μ.Σ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΚΙΝΔΥΝΟΙ ΚΑΙ ΑΠΑΙΤΗΣΕΙΣ ΣΕ ΣΥΣΤΗΜΑΤΑ ΑΝΕΠΑΦΩΝ ΣΥΝΑΛΛΑΓΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων: Λαμπρινουδάκης Κωνσταντίνος

Καθηγητής ΠΑ.ΠΕΙ

Αθήνα, Νοέμβριος 2019

Περίληψη

Καθημερινά πραγματοποιείται τεράστιος αριθμός συναλλαγών. Ειδικότερα τα τελευταία χρόνια, μεγάλο μέρος αυτών καλύπτουν οι ανέπαφες συναλλαγές. Οι ανέπαφες συναλλαγές βασίζονται στην ασύρματη τεχνολογία μικρής εμβέλειας NFC (Near Field Communication) και πραγματοποιούνται πλησιάζοντας την κάρτα contactless στο ειδικό τερματικό αποδοχής καρτών. Πρόκειται για μια ιδανική τεχνολογία όταν η ταχύτητα στην εξυπηρέτηση αλλά και η ευκολία έχουν μεγάλη σημασία. Ακριβώς λόγω της εκτεταμένης χρήσης τους, καθίσταται απαραίτητη η μελέτη σχετικά με την ασφάλεια των συστημάτων που διαχειρίζονται τέτοιου είδους συναλλαγές.

Στην παρούσα διπλωματική εργασία, σκοπός μας ήταν η μελέτη της αρχιτεκτονικής και του λειτουργικού συστήματος των έξυπνων καρτών (άρα κατ' επέκταση των χρεωστικών/πιστωτικών καρτών) αλλά και των τερματικών EFT/POS. Εξετάζεται επίσης η ανέπαφη λειτουργία, ο τρόπος πραγματοποίησης της ασύρματης ζεύξης και οι ευπάθειες που προκύπτουν από τη χρήση της ασύρματης τεχνολογίας. Στο πειραματικό κομμάτι, έγιναν προσπάθειες επιθέσεων τύπου Eavesdropping και Jamming με τη χρήση αυτοσχέδιας κεραίας. Τέλος, εξετάζονται κάποιες προτάσεις ασφάλειας σε επίπεδο υλικού και λογισμικού.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τον κ. Λαμπρινουδάκη για την ευκαιρία που μου έδωσε να ασχοληθώ με το συγκεκριμένο θέμα μιας και αποτελεί ένα ιδιαίτερα επίκαιρο πεδίο δεδομένης της ευρείας χρήσης των πιστωτικών/χρεωστικών καρτών στις μέρες μας.

Θα ήθελα επίσης να ευχαριστήσω τον κ. Κανάτα και το εργαστήριο Δικτύων και Τηλεπικοινωνιών του τμήματος Ψηφιακών Συστημάτων, Πανεπιστημίου Πειραιώς αφού χωρίς τον εξοπλισμό που μου παρείχαν, δε θα μπορούσα να υλοποιήσω το πειραματικό μέρος της διπλωματικής εργασίας.

Επίσης, ευχαριστώ ιδιαιτέρως τους συναδέλφους μου από το τμήμα του POS Development για τον εξοπλισμό, το χρόνο, αλλά και το χώρο που μου αφιέρωσαν για τη διεξαγωγή των πειραμάτων.

Ένα μεγάλο ευχαριστώ στην οικογένειά μου και τους φίλους μου για τη συνεχή στήριξη τους. Τέλος, το μεγαλύτερο ευχαριστώ το οφείλω στο Χρήστο για τη βοήθεια που μου παρείχε σε όλη τη διάρκεια αλλά και την παρότρυνσή του.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 1ο - ΕΙΣΑΓΩΓΗ

1.1 Η ΣΗΜΑΣΙΑ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ ΣΤΙΣ ΣΥΝΑΛΛΑΓΕΣ

Καθημερινά διεκπεραιώνονται εκατομμύρια πληρωμές σε όλο τον κόσμο. Οι πληρωμές αυτές γίνονται μεταξύ μεμονωμένων ανθρώπων και νομικών προσώπων με όλους τους δυνατούς συνδυασμούς και δε γνωρίζουν σύνορα. Η πληρωμή, ανεξάρτητα της στάσης ζωής κάθε ανθρώπου, δεν παύει να είναι απαραίτητη προϋπόθεση για την ικανοποίηση των αναγκών μας.

Ο καταναλωτής αξιοποιεί τεχνολογικά μέσα για να ολοκληρώσει την πληρωμή και ο ίδιος ο δικαιούχος αξιοποιεί παρόμοια τεχνολογικά μέσα για να βεβαιωθεί για την ολοκλήρωσή της και να τη θεωρήσει ως είσπραξη. Υπάρχουν διάφορες μέθοδοι πληρωμών, όπως οι πληρωμές στα ταμεία των τραπεζών, οι πληρωμές στα μηχανήματα ATM, οι ηλεκτρονικές πληρωμές αλλά και οι πληρωμές με χρεωστική ή πιστωτική κάρτα σε τερματικό EFT/POS (Electronic Funds Transfer/Point of Sales). Οι πληρωμές με χρεωστική ή πιστωτική κάρτα σε τερματικό EFT/POS ανήκουν στην κατηγορία των ηλεκτρονικών συναλλαγών ωστόσο γίνονται πρόσωπο-με-πρόσωπο την ώρα της εμπορικής συναλλαγής.

Κάθε επιχείρηση μπορεί να συνεργαστεί με μία ή περισσότερες τράπεζες και να αποκτήσει τη δυνατότητα να κάνει τις εισπράξεις της, χρεώνοντας οποιαδήποτε πιστωτική/χρεωστική κάρτα που φέρει το σήμα ενός από τους διεθνείς οργανισμούς καρτών (Visa, MasterCard, Diners, American Express) και ανεξάρτητα από τη χώρα και την τράπεζα που έχει εκδώσει την κάρτα. Το τερματικό EFT/POS ανήκει στην τράπεζα με την οποία συνεργάζεται το εκάστοτε κατάστημα. [1]

Ειδικότερα, οι ανέπαφες συναλλαγές αποτελούν το νέο εύκολο και γρήγορο τρόπο για την πραγματοποίηση αγορών με χρήση καρτών ειδικής τεχνολογίας, οι οποίες φέρουν συγκεκριμένο σήμα (βλ. Σχήμα 1.1). Η διαδικασία πληρωμής με τις κάρτες ανέπαφων συναλλαγών, είναι γρηγορότερη από την αντίστοιχη διαδικασία πληρωμής με μετρητά ή ενσύρματα με κάρτα, με αποτέλεσμα να μειώνεται ο χρόνος αναμονής και η ουρά στο ταμείο καθώς οι συναλλαγές ολοκληρώνονται σε ελάχιστα δευτερόλεπτα. Οι έξυπνες συσκευές μπορούν να αποθηκεύουν σε ένα εικονικό «πορτοφόλι» τα στοιχεία διαφόρων καρτών που υποστηρίζουν τις ανέπαφες συναλλαγές και με αυτόν τον τρόπο, ο αγοραστής να επιλέγει την κάρτα της προτίμησής του για την πραγματοποίηση της συναλλαγής.

Σχήμα 1.1: Ένδειξη η οποία δηλώνει υποστήριξη ανέπαφης συναλλαγής

1.2 Η ΔΙΑΔΙΚΑΣΙΑ ΣΥΝΑΛΛΑΓΗΣ

Οι ανέπαφες συναλλαγές, όπως μαρτυρά η ονομασία τους, είναι αυτές που γίνονται χωρίς επαφή. Πρόκειται για έναν εύκολο και γρήγορο τρόπο για να πραγματοποιήσει κάποιος τις πληρωμές του με τις λεγόμενες ασύρματες τραπεζικές κάρτες. Για την πληρωμή, απλά πρέπει η κάρτα (πιστωτική ή χρεωστική) να πλησιάσει στο τερματικό EFT/POS με την προϋπόθεση πως τόσο η κάρτα, όσο και το μηχάνημα υποστηρίζουν τη συγκεκριμένη τεχνολογία. Ο κάτοχος του τερματικού EFT/POS εισάγει το ποσό πληρωμής, το οποίο και εμφανίζεται στην οθόνη του μηχανήματος αποδοχής καρτών και ο πελάτης, απλά πλησιάζει την χρεωστική/πιστωτική κάρτα στο κατάλληλο μηχάνημα. Για την πραγματοποίηση της συναλλαγής πρέπει να έχει προηγηθεί η πληκτρολόγηση του ποσού της αγοράς από τον έμπορο στο μηχάνημα αποδοχής καρτών. Επομένως, όσες φορές κι αν περάσει η κάρτα μπροστά από το μηχάνημα, δε θα υπάρξει χρέωση αφού το μηχάνημα δεν έχει «προετοιμαστεί» για να υποδεχθεί οποιαδήποτε συναλλαγή. Σε ελάχιστα δευτερόλεπτα ακούγεται ένας χαρακτηριστικός ήχος και εμφανίζεται ένδειξη έγκρισης στην οθόνη του τερματικού EFT/POS. Ο έμπορος παραδίδει το απόκομμα της συναλλαγής που εκδίδεται από το μηχάνημα.

Όσον αφορά τις μικροσυναλλαγές, για λόγους διευκόλυνσης, δε απαιτούν την εισαγωγή κωδικού PIN. Το όριο συναλλαγών έχει οριστεί από τους Διεθνείς Οργανισμούς Visa και MasterCard και δεν υπάρχει δυνατότητα αλλαγής ή κατάργησής του. Οι κάρτες που υποστηρίζουν ανέπαφες συναλλαγές, υποστηρίζουν επίσης τη σύγχρονη τεχνολογία ασφαλείας Chip & PIN. Επομένως, κατά την πραγματοποίηση της συναλλαγής, ο αγοραστής μπορεί να απαιτήσει να γίνει εισαγωγή της κάρτας του στην ειδική υποδοχή του τερματικού EFT/POS και να πληκτρολογήσει τον τετραψήφιο κωδικό PIN. [2]

Μια ανέπαφη συναλλαγή μπορεί να διαιρεθεί σε τρία συστήματα, την κάρτα, το τερματικό EFT/POS και την ασύρματη ζεύξη μεταξύ των δυο. Εν τάχει:

Η κάρτα ενσωματώνει ένα Chip και μία κεραία που ανταποκρίνεται στο αίτημα του POS

τερματικού σταθμού χρησιμοποιώντας ένα εύρος συχνοτήτων 13,56 MHz.

Όσον αφορά το μηχάνημα πληρωμών EFT/POS πρόκειται για μία ηλεκτρονική συσκευή που χρησιμοποιείται για την επεξεργασία των συναλλαγών μέσω κάρτας πληρωμών. Ένα τερματικό EFT/POS πραγματοποιεί τις εξής λειτουργίες:

- Διαβάζει και επεξεργάζεται τις πληροφορίες από την πιστωτική ή χρεωστική κάρτα. Συγκεκριμένα, λαμβάνει το όνομα του κατόχου της κάρτας και τον αριθμό λογαριασμού. Αποθηκεύει τις πληροφορίες όπως τον αριθμό της κάρτας πληρωμής και την ημερομηνία λήξης της.
- Ελέγχει εάν τα χρήματα του τραπεζικού λογαριασμού του πελάτη επαρκούν για τη συναλλαγή
- Μεταφέρει τα χρήματα από το λογαριασμό του πελάτη στο λογαριασμό του πωλητή (συγκεκριμένα τους λογαριασμούς για τη μεταφορά του ποσού με το δίκτυο της πιστωτικής/χρεωστικής κάρτας)
- Καταγράφει τη συναλλαγή και εκτυπώνει την απόδειξη

Οι ανέπαφες συναλλαγές βασίζονται στην ασύρματη τεχνολογία μικρής εμβέλειας NFC (Near Field Communication). Πρόκειται για μία αμφίδρομη, μικρής εμβέλειας (έως 10cm) τεχνολογία ανέπαφων επικοινωνιών βασισμένη στα πρότυπα ISO-14443 και Sony FeLiCa (RFID). [5] Λειτουργεί στο φάσμα των 13,56 MHz και υποστηρίζει ταχύτητες μεταφοράς δεδομένων 106, 216 και 424 kbps. Επιτρέπει στις συσκευές που τη διαθέτουν, να επικοινωνούν με ασύρματο τρόπο με τις άλλες συσκευές που βρίσκονται εντός εμβέλειας. Ο αναγνώστης, στην ουσία, θα πρέπει να βρίσκεται σε άμεση γειτνίαση με την κάρτα. Τα διαφορετικά συστήματα πληρωμών χρησιμοποιούν τα δικά τους πρότυπα που ονομάζονται Visa payWave, MasterCard PayPass, American Express ExpressPay κλπ. Παρόλα αυτά, όλοι οι κατασκευαστές εξακολουθούν να χρησιμοποιούν την ίδια προσέγγιση και την ίδια βασική τεχνολογία.

Πέραν των τραπεζικών καρτών, όπως ειπώθηκε και παραπάνω, μπορούν να χρησιμοποιηθούν και τα έξυπνα κινητά (εάν ο ενδιαφερόμενος διαθέτει κάποια εφαρμογή πορτοφολιού - wallet), το smartwatch ή ακόμα και τα ειδικά βραχιολάκια (smartbands) που έχουν αρχίσει να διαθέτουν ήδη στους πελάτες τους ορισμένες τράπεζες.

Σχήμα 1.2: Τεχνολογικά μέσα (πιστωτική/χρεωστική κάρτα, έξυπνη συσκευή, smartwatch) για την πραγματοποίηση ανέπαφων συναλλαγών

1.3. ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΑΝΕΠΑΦΕΣ ΣΥΝΑΛΛΑΓΕΣ

Οι ανέπαφες συναλλαγές προσφέρουν ταχύτητα και ευκολία και έτσι η χρήση τους είναι ιδιαίτερα διαδεδομένη. Ενδεικτικά αναφέρουμε πως σύμφωνα με τελευταίες μελέτες της Mastercard, η Ελλάδα αποτελεί μία από τις ταχύτερα αναπτυσσόμενες αγορές στις ανέπαφες συναλλαγές, με ιδιαίτερα εντυπωσιακό ποσοστό 58% των συνολικών συναλλαγών να διεκπεραιώνονται ανέπαφα, καταγράφοντας αύξηση υψηλότερη από 180%, τον τελευταίο χρόνο. [3]

Ακριβώς λόγω της εκτεταμένης χρήσης τους, καθίσταται απαραίτητη η μελέτη σχετικά με την ασφάλεια των συστημάτων που διαχειρίζονται τέτοιου είδους συναλλαγές. Για τις ανέπαφες συναλλαγές, ο χρηματοπιστωτικός κλάδος χρησιμοποιεί προηγμένες τεχνολογίες ασφάλειας τόσο όσον αφορά την κάρτα όσο και στο τερματικό EFT/POS αλλά και δίκτυο επικοινωνίας και επεξεργασίας των δεδομένων αυτών με σκοπό την πρόληψη πιθανής απάτης.

Ωστόσο, σύμφωνα με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η χρήση

χρεωστικών καρτών ανέπαφων συναλλαγών κρύβει σοβαρούς κινδύνους για τους κατόχους τους, αφενός γιατί σε περίπτωση απώλειας η κάρτα μπορεί να περιέλθει στα χέρια τρίτου, ο οποίος θα μπορεί να τη χρησιμοποιεί για αγορές ως 25 ευρώ η κάθε μία χωρίς να είναι απαραίτητο να γνωρίζει το pin και αφετέρου γιατί μια τέτοια κάρτα, εκπέμπει μέσω ραδιοκυμάτων υψηλής συχνότητας, κάτι που σημαίνει πως κάποιος με την κατάλληλη συσκευή ανάγνωσης μπορεί να καταγράψει προσωπικά δεδομένα όπως τον αριθμό και την ημερομηνία λήξης της.[4] Η τεχνολογία NFC έχει αποδειχθεί ευάλωτη σε διάφορες απειλές, όπως η υποκλοπή (eavesdropping), η τροποποίηση δεδομένων (data modification) αλλά και σε επιθέσεις αναμετάδοσης (relay attacks). Επόμενο είναι λοιπόν να προκύπτουν ερωτήματα γύρω από την επάρκεια των μέτρων στα συστημάτων ασφάλειας που λαμβάνονται.

1.4 ΣΤΟΧΟΣ ΚΑΙ ΔΟΜΗ ΤΗΣ ΕΡΓΑΣΙΑΣ

Στόχο της εργασίας αποτελεί η μελέτη της λειτουργίας των καρτών που υποστηρίζουν την τεχνολογία ανέπαφων συναλλαγών, των τερματικών EFT/POS αλλά και της τεχνολογίας που χρησιμοποιείται για την μεταξύ τους επικοινωνία. Τα παραπάνω πραγματοποιούνται, με απώτερο σκοπό την ανάλυση των κινδύνων και εύρεση ευπαθειών αλλά και την εξαγωγή συμπερασμάτων σχετικά με την ασφάλεια των ανέπαφων συναλλαγών.

Η παρούσα διπλωματική εργασία αποτελείται από δυο μέρη, με το πρώτο μέρος να είναι θεωρητικό ενώ το δεύτερο πειραματικό.

Στο πρώτο αναλύεται η αρχιτεκτονική των έξυπνων καρτών (άρα κατ’ επέκταση των χρεωστικών/πιστωτικών καρτών) αλλά και το λειτουργικό σύστημα αυτών. Ακόμη, μελετάται η αρχιτεκτονική και η λειτουργία του τερματικού EFT/POS. Στη συνέχεια, εξετάζεται η διαδικασία της συναλλαγής, σχετικά με τον τρόπο επικοινωνίας των συστημάτων, τα πρωτόκολλα που χρησιμοποιούνται, αλλά και τη κρυπτογράφηση. Εξετάζεται επίσης η ανέπαφη λειτουργία, συγκεκριμένα εντοπίζονται οι διαφορές της με την τεχνολογία εξ’ επαφής, τον τρόπο πραγματοποίησης της ασύρματης ζεύξης, τις ευπάθειες που προκύπτουν από τη χρήση της ασύρματης τεχνολογίας αλλά και τις γνωστές επιθέσεις, που βρίσκονται στη βιβλιογραφία.

Στο δεύτερο μέρος παρουσιάζονται κάποια πειράματα που πραγματοποιήθηκαν, με σκοπό την εκμετάλλευση των ευπαθειών σε συστήματα ανέπαφων συναλλαγών.

Τέλος, παρατίθεται η βιβλιογραφία και οι πηγές που χρησιμοποιήθηκαν κατά τη συγγραφή της διπλωματικής εργασίας.

ΚΕΦΑΛΑΙΟ 2^{ο} - ΕΞΥΠΝΕΣ ΚΑΡΤΕΣ

Σε αυτό το κεφάλαιο μελετούνται οι έξυπνες κάρτες, οι οποίες αποτελούν στην ουσιά ένα ενσωματωμένο υπολογιστικό σύστημα και ως τέτοιο μελετάται σε επίπεδο φυσικό/υλικό, αρχιτεκτονικής και λειτουργικού συστήματος/filesystem.

2.1 ΚΑΤΗΓΟΡΙΕΣ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

Οι κάρτες, ανάλογα με τη λειτουργία την οποία πραγματοποιούν και τα χαρακτηριστικά που διαθέτουν, διακρίνονται στις παρακάτω κατηγορίες:

- MEMORY CARDS
  Αυτές οι κάρτες περιέχουν μόνο μνήμη που μπορεί να αρχικοποιηθεί μία φορά και διαθέτει ελάχιστα χαρακτηριστικά ασφαλείας. Αυτές οι κάρτες μπορούν να χρησιμοποιηθούν σε συστήματα όπου ορίζεται μία συγκεκριμένη τιμή και αποθηκεύεται στη κάρτα, όπως προπληρωμένες τηλεφωνικές κάρτες. Σε άλλες εφαρμογές στη κάρτα περιέρχεται απλά ένα αναγνωριστικό που συνδέεται με δεδομένα στο back end ενός συστήματος. Αυτές οι κάρτες έχουν περιορισμένη λειτουργικότητα και συχνά αχρηστεύονται μετά τη χρήση τους.

- MEMORY CARDS WITH LOGIC
  Πρόκειται για μία πιο ευέλικτη έκδοση της κάρτας μνήμης στην οποία υλοποιείται λογική που ελέγχει την πρόσβαση στη μνήμη της κάρτας. Αυτή η δυνατότητα, δίνει στον εκδότη της κάρτας περισσότερη ελευθερία για την τροποποίηση ή ενημέρωση των δεδομένων, που είναι αποθηκευμένα στη μνήμη της κάρτας, π.χ. επαναφόρτιση μίας προπληρωμένης τηλεφωνικής κάρτας. Αυτό επιτρέπει τη λειτουργία πιο σύνθετων εφαρμογών και επιμηκύνει τη διάρκεια ζωής της κάρτας.

- MICROPROCESSOR CARDS
  Σε αυτή την κατηγορία ανήκουν οι έξυπνες κάρτες που μπορούν να υποστηρίξουν πιο περίπλοκα συστήματα καθώς διαθέτουν μικροεπεξεργαστή. Περιέχουν λειτουργικό σύστημα και επιτρέπουν στον εκδότη να προσδιορίσει τις δικές του εντολές, τη λειτουργικότητα και τις δομές δεδομένων. Οι πληροφορίες για τον πελάτη αποθηκεύονται σε προγραμματιζόμενη μη πτητική μνήμη, όπως π.χ. Flash ή EEPROM (Electrically Erasable Programmable Read Only Memory), η οποία μπορεί να

τροποποιηθεί από την έξυπνη κάρτα. Οι πιο συνηθισμένες χρήσεις τέτοιων έξυπνων καρτών είναι οι τραπεζικές κάρτες και οι SIM (Subscriber Identity Modules) κάρτες για κινητά τηλέφωνα.

Κατηγοριοποιούνται επίσης, ανάλογα με τις διεπαφές επικοινωνίας τις οποίες διαθέτουν στις:

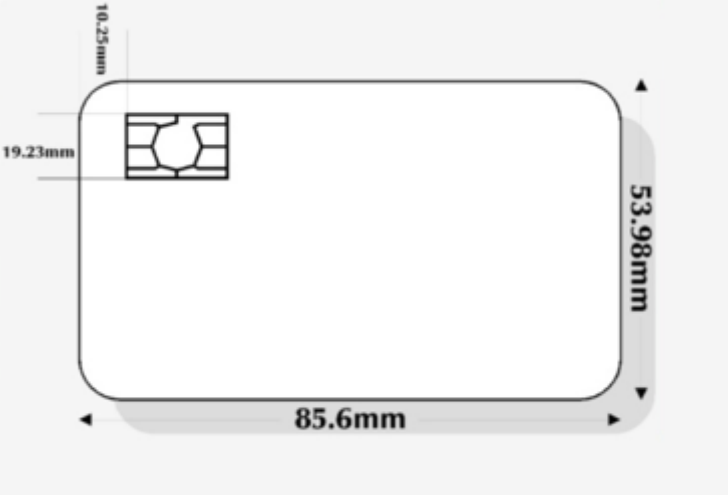
- Επαφής(*Contact*)
- Ανέπαφες (*Contactless*)

  Η διαφορά των δυο παραπάνω είναι η μέθοδος επικοινωνίας, όπου στις πρώτες επιτυγχάνεται με την εισαγωγή της κάρτας στον αναγνώστη και την επαφή των ακροδεκτών τους, ενώ στις δεύτερες ασύρματα μέσω κεραίας εντός του πλαστικού σώματος της κάρτας.
  Όσο αφορά τις ανέπαφες κάρτες, υπάρχουν δύο τύποι: οι κάρτες εγγύτητας (vicinity cards) (Πρότυπο ISO 2000a) και έχουν εμβέλεια επικοινωνίας μέχρι ένα μέτρο, και οι κάρτες μεγάλης εγγύτητας (proximity cards) (Πρότυπο ISO 2000b) οι οποίες έχουν εύρος περίπου δέκα εκατοστά. Η ασύρματη διασύνδεση προσφέρει στους αναγνώστες και τις έξυπνες κάρτες μεγαλύτερη διάρκεια ζωής σε σύγκριση με τους αναγνώστες καρτών επαφής. Αυτό συμβαίνει επειδή δεν υπάρχει φθορά που προκαλείται στις επαφές από την επανειλημμένη εισαγωγή κάρτας στον αναγνώστη.

- Υβριδικές (*Dual Interface - Combi*)
  Ορισμένες έξυπνες κάρτες έχουν την δυνατότητα να επικοινωνούν και με τους δυο παραπάνω τρόπους. Είναι συνήθως σχεδιασμένες για να υποστηρίζουν περισσότερες από μία εφαρμογές, π.χ. την πληρωμή με χρήση της κάρτας εξ' επαφής και την έκδοση εισιτηρίων ανέπαφα.[9]

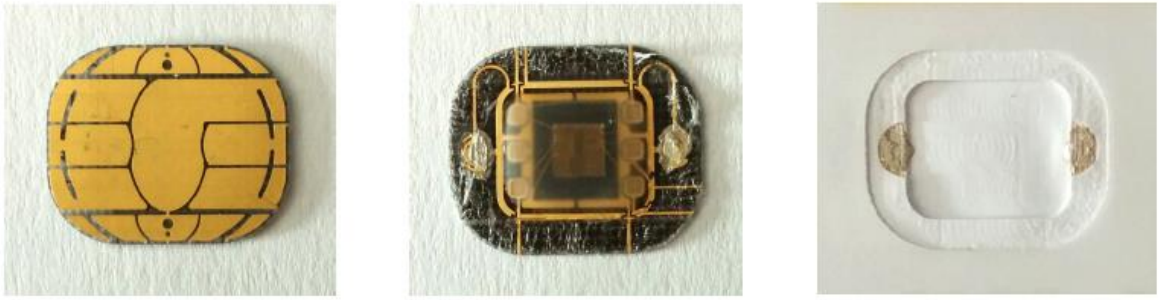
2.2 Η ΦΥΣΙΚΗ ΕΜΦΑΝΙΣΗ ΤΗΣ ΚΑΡΤΑΣ

Μία τραπεζική κάρτα, είτε χρεωστική είτε πιστωτική, είναι μία λεπτή πλαστική κάρτα, συνήθως με διαστάσεις 85.6mm x 53.98mm x 0.76mm (βλ. Σχήμα 2.1), όπως καθορίζεται και μέσω του ISO προτύπου 7816. Ονομάζεται επίσης και κάρτα ολοκληρωμένου κυκλώματος (Integrated Circuit Card, ICC) αφού διαθέτει ενσωματωμένο μικροεπεξεργαστή καθώς και κύκλωμα, κατάλληλο για την αποθήκευση δεδομένων.



Σχήμα 2.1: Διαστάσεις έξυπνης κάρτας

Οι τραπεζικές κάρτες έχουν τυποποιημένα χαρακτηριστικά: πολλαπλές στρώσεις (συνήθως 4 έως 5 στρώματα ατομικών πλαστικών φύλλων) με τυπωμένο σχέδιο και προαιρετικά χαρακτηριστικά ασφαλείας, μαγνητική ταινία, ολόγραμμα και ολοκληρωμένο κύκλωμα με τους ακροδέκτες του.



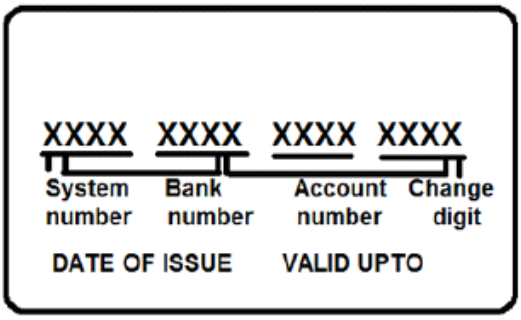
Σχήμα 2.2. Οι ακροδέκτες (αριστερά) το ολοκληρωμένο κύκλωμα (κέντρο) και η εσοχή που το συγκρατεί στο σώμα της κάρτας (δεξιά)

Η οπτική εξατομίκευση της κάρτας γίνεται είτε με ανάγλυφη εκτύπωση είτε με χάραξη με χρήση λέιζερ.

Εξωτερικά φέρει στοιχεία ταυτοποίησης όπως, όνομα και επώνυμο δικαιούχου, αριθμό κάρτας, ημερομηνία έκδοσης, ημερομηνία λήξης, αλλά και τον αριθμό επαλήθευσης (CVV).

Ουσιαστικά, εξουσιοδοτεί τον δικαιούχο (το άτομο του οποίου το όνομα αναγράφεται πάνω στην κάρτα) να τη χρησιμοποιήσει για αγορές, αναλήψεις κ.λπ. και διαβάζεται από μηχανήματα ATM, τερματικά EFT/POS κ.α.

Ο αριθμός της κάρτας, αποτελείται από δεκαέξι (16) ψηφία, τα οποία κατηγοριοποιημένα ανά τέσσερις (4) ομάδες, αντιπροσωπεύουν μία συγκεκριμένη λεπτομέρεια (βλ. Σχήμα 2.3).



Σχήμα 2.3: Αριθμός κάρτας

Το πρώτο ψηφίο (Major Industry Identifier, MII) υποδηλώνει την ευρύτερη κατηγορία στην οποία ανήκει η εταιρεία ή ο Οργανισμός που εξέδωσε την κάρτα (π.χ. Χρηματοπιστωτικά Ιδρύματα, Αεροπορικές Εταιρείες, Τηλεπικοινωνίες, κ.α.). Συγκεκριμένα, τα ψηφία 4 ή 5 υποδεικνύουν τραπεζικό/χρηματοοικονομικό ίδρυμα και το ψηφίο 6, Εμπορικό οργανισμό ή τραπεζικό/χρηματοοικονομικό ίδρυμα. Τα πρώτα 6 ή 7 ψηφία φανερώνουν τον εκδότη της κάρτας και ο αριθμός αυτός ονομάζεται Issuer Identification Number (IIN). Ο αριθμός αυτός είναι κοινός για όλες τις ίδιου τύπου κάρτες που έχουν εκδοθεί από το ίδιο ίδρυμα. Τα ψηφία από το 7^{ο} (ή 8ο) έως το 15ο είναι ο προσωπικός λογαριασμός του κατόχου της κάρτας. Το 16ο ψηφίο, δηλαδή το τελευταίο είναι το ψηφίο επαλήθευσης και χρησιμοποιείται για να επαληθευτεί η γνησιότητα της κάρτας με τον αλγόριθμο Luhn.

2.3 ΜΑΓΝΗΤΙΚΗ ΛΩΡΙΔΑ

Οι κάρτες όπως αναφέρθηκε και στα παραπάνω, διαθέτουν μία μαγνητική λωρίδα. Αποτελείται από μικροσκοπικά μαγνητικά σωματίδια από σίδηρο σε μία πλαστική μεμβράνη. Η μαγνητική λωρίδα αποθηκεύει πληροφορίες αλλάζοντας το μαγνητικό πεδίο της. Διαθέτει χωρητικότητα αποθήκευσης περίπου 200 χαρακτήρων. Οι πληροφορίες που αποθηκεύονται είναι μόνο για ανάγνωση, χωρίς υπολογιστική ισχύ.

Η μαγνητική λωρίδα φθείρεται αλλά και διαταράσσεται εύκολα από άλλα μαγνητικά πεδία. Το σημαντικό πράγμα που πρέπει να ειπωθεί για τις κάρτες μαγνητικής ταινίας είναι ότι δεν είναι

έξυπνες κάρτες επειδή αποτυγχάνουν να ικανοποιήσουν τις συνθήκες που θέτονται από τον ορισμό αυτών.[6][7]

2.4 ΕΝΣΥΡΜΑΤΗ ΔΙΕΠΑΦΗ

Στην ενσύρματη διεπαφή έχουμε την εισαγωγή της κάρτας στο τερματικό. Μέσω αυτού γίνεται η σειριακή επικοινωνία τύπου half duplex μέσω της θύρας εισόδου εξόδου. Επιπρόσθετα η συσκευή είναι υπεύθυνη και για την τροφοδοσία του κυκλώματος της κάρτας.

Οι κάρτες διαθέτουν συνολικά οκτώ ακροδέκτες, εξ αυτών χρησιμοποιούνται ευρέως οι έξι, ενώ οι υπόλοιποι δύο προορίζονται για μελλοντική χρήση. Σε ειδικές κάρτες δοκιμών ή εντοπισμού σφαλμάτων, αυτοί οι ακροδέκτες έχουν ενίοτε λειτουργικότητα ανάλογα με την συγκεκριμένη εφαρμογή. Στο παρακάτω πίνακα δίνεται μια σύντομη περιγραφή των ακροδεκτών:

Όνομα ακροδέκτη	Περιγραφή λειτουργίας
1.Τροφοδοσία- VCC	Το τερματικό EFT/POS πρέπει να παρέχει τάση είτε 5.0V, 3.0V ή 1.8V σε αυτόν τον ακροδέκτη για να τροφοδοτήσει την έξυπνη κάρτα.
2.Επαναφορά - RST	Ο ακροδέκτης επαναφοράς μπορεί να χρησιμοποιηθεί για την επαναφορά της έξυπνης κάρτας.
3.Ρολόι - CLK	Εάν η έξυπνη κάρτα δεν διαθέτει εσωτερικό ρολόι, το τερματικό EFT/POS πρέπει να παρέχει ένα σήμα ρολογιού συχνότητας 3Mhz έως 5Mhz σε αυτόν τον ακροδέκτη.
4 και 8. Μελλοντικής χρήσης - RFU	Οι δυο αυτοί ακροδέκτες προορίζονται για μελλοντική/ειδική χρήση.
5.Γείωση – GND	Το τερματικό EFT/POS παρέχει τάση αναφοράς σε αυτόν τον ακροδέκτη
6.Προγραμματισμού – VPP	Χρησιμοποιείται για παροχή τάσης απαραίτητη για τον προγραμματισμό ή διαγραφή/εγγραφή στη μη-πτητική μνήμη.
7.Είσοδος/Εξόδος – I / O	Η επικοινωνία μεταξύ της κάρτας και του τερματικού EFT/POS πραγματοποιείται μέσω αυτού του ακροδέκτη.[8]

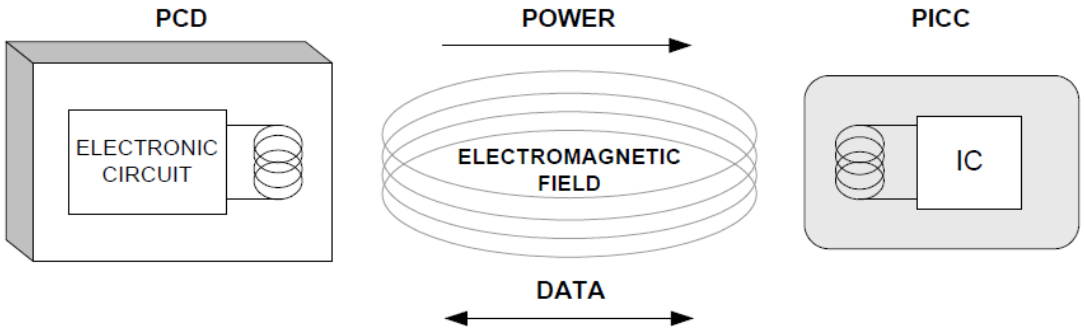
Σχήμα 2.4: Ακροδέκτες σε κάρτες επαφής[10]

2.5 ΑΣΥΡΜΑΤΗ ΔΙΕΠΑΦΗ

Οι ασύρματες κάρτες στην ασύρματη διεπαφή τροφοδοτούνται και επικοινωνούν με το τερματικό ασύρματα μέσω ηλεκτρομαγνητικής επαγωγής. Για αυτό το σκοπό διαθέτουν κεραία συνήθως τυπωμένη από λεπτό στρώμα χαλκού λίγων περιελίξεων (στη βιβλιογραφία βρίσκεται τυπικός αριθμός πέντε περιελίξεων) [8].

Σχήμα 2.5 Σχέδιο κεραίας σε κάρτα Visa της Austria Card [8]

Ο συνδυασμός της συσκευής ανάγνωσης (Proximity Coupling Device) και της κάρτας (Proximity IC Card) λειτουργεί ουσιαστικά σαν μετασχηματιστής με το πρωτεύον πηνίο να βρίσκεται στη πρώτη συσκευή και το δεύτερο στην κάρτα [10]. Με αυτόν τον τρόπο, σε κοντινή απόσταση γίνεται η μεταφορά ενέργειας μέσω αέρα.



Σχήμα 2.6 Μεταφορά ενέργειας και ανταλλαγή πληροφοριών PCD-PICC [10]

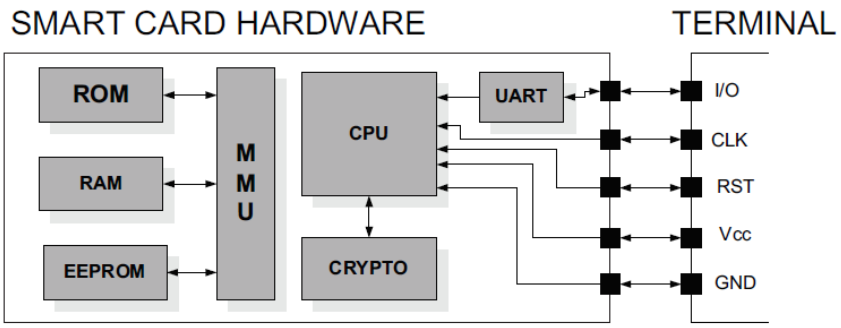
Συγκεκριμένα, με μεθόδους διαμόρφωσης έχουμε RF σήμα κατάλληλο όχι μόνο για την επικοινωνία μεταξύ των δυο συστημάτων αλλά και για την τροφοδοσία της κάρτας.

Από τα παραπάνω προκύπτει η ανάγκη για επιπλέον υλικό στις ασύρματες κάρτες για την ανόρθωση του εναλλασσόμενου σήματος, την παραγωγή σταθερής τάσης τροφοδοσίας καθώς και για την αποδιαμόρφωση του σήματος[9]. Αυτά τα επιπρόσθετα ηλεκτρονικά που δεν υπάρχουν στις κάρτες επαφής, έχουν φυσικά σαν αποτέλεσμα συγκριτικά μεγαλύτερο κόστος παραγωγής των ασύρματων καρτών έναντι των προηγουμένων.

2.6 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ

Την καρδιά της έξυπνης κάρτας αποτελεί η κεντρική επεξεργαστική μονάδα (CPU) και πλαισιώνεται από τέσσερα λειτουργικά τμήματα, την μνήμη ROM, EEPROM, RAM και τη θύρα I/O. Επιπρόσθετα περιλαμβάνεται και ειδικό υλικό για κρυπτογράφηση (CRYPTO) και την διαχείριση της μνήμης (MMU).

Αναλυτικότερα στη ROM περιέχεται το λειτουργικό σύστημα το οποίο εγγράφεται κατά την παραγωγή. Η ROM χρησιμοποιείται επίσης για την αποθήκευση σταθερών δεδομένων και ρουτινών καθώς και πινάκων αντιστοίχισης. Είναι αποδοτική από άποψη χώρου και κατανάλωσης πόρων και το περιεχόμενο της παραμένει στατικό καθ’ όλη την διάρκεια ζωής της κάρτας, χωρίς δυνατότητα αλλαγής.



Σχήμα 2.7 Αρχιτεκτονική έξυπνης κάρτας

Η RAM είναι η λειτουργική μνήμη του συστήματος. Είναι πτητική μνήμη που χρησιμοποιείται για προσωρινή αποθήκευση κατά την εκτέλεση προγραμμάτων. Αποτελεί τον πολυτιμότερο πόρο από τη πλευρά της ανάπτυξης λογισμικού λόγω του περιορισμένου μεγέθους και αυξημένης κατανάλωσης της. Όταν ξεπερνιέται η χωρητικότητα της τα δεδομένα της περνάνε στη EEPROM.

Η μνήμη EEPROM είναι ένα ακριβή και καταλαμβάνει μεγάλη επιφάνεια στο τσιπ, επιπλέον η οργάνωση της είναι αρκετά περίπλοκη. Η πρώτη περιοχή της (manufacturing data region) περιέχει κατασκευαστικά δεδομένα, η δεύτερη (OS region) πίνακες και δείκτες που μαζί με τις ρουτίνες τις ROM συνθέτουν το πλήρες λειτουργικό σύστημα. Οι επόμενες περιοχές, (application program region και file region) περιέχουν συγκεκριμένες εντολές και αλγορίθμους που δεν χωράνε στη ROM και το σύστημα οργάνωσης των αρχείων αντίστοιχα. Τέλος μπορεί να υπάρχει ελεύθερη περιοχή μνήμης που χρησιμοποιείται από συγκεκριμένες εφαρμογές. Γενικότερα η EEPROM έχει αρκετά μακρύ χρόνο προσπέλασης και περιορισμένο αν και μεγάλο αριθμό κύκλων εγγραφής.

Η θύρα I/O συνδέεται με τη CPU μέσω του κατάλληλου υλικού (Universal Asynchronous Receiver Transmitter) για την σειριοποίηση των εντολών που έρχονται από το τερματικό και τις απαντήσεις προς αυτό.

Τέλος ο κρυπτο-επεξεργαστής είναι ένας δεύτερος ειδικού σκοπού επεξεργαστής που εκτελεί αποδοτικά ένα πολύ περιορισμένο αριθμό κρυπτογραφικών εντολών. Η εισαγωγή τέτοιου ειδικού υλικού εξοικονομεί επίσης πόρους, καθώς η κρυπτογράφηση είναι ένα πολύ μεγάλο μέρος των λειτουργιών του συνολικότερου συστήματος.

2.7 ΛΟΓΙΣΜΙΚΟ ΤΩΝ ΕΞΥΠΝΩΝ ΚΑΡΤΩΝ (SOFTWARE)

Οι έξυπνες κάρτες μπορούν να διαθέτουν μια ποικιλία εφαρμογών. Οι εφαρμογές αυτές οργανώνονται ως αρχεία και φάκελοι στην κάρτα. Η δομή μπορεί να συγκριθεί με τα συστήματα αρχείων του λειτουργικού συστήματος Linux.

Το σύστημα οργάνωσης αρχείων (filesystem) αποτελείται από τριών ειδών αρχεία:

- κύριο αρχείο (MF - Master File),
- ειδικά αρχεία (DF – Dedicated Files) και
- στοιχειώδη αρχεία (EF- Elementary Files).

Το MF είναι η ρίζα της δομής και περιέχει όλα τα DFs και EFs. Τα DFs λειτουργούν ως φάκελοι και περιέχουν άλλα χαμηλότερου επιπέδου EFs και DFs τα οποία ανήκουν μαζί με λογικό τρόπο. Τα EFs είναι αρχεία τα οποία περιέχουν δεδομένα και είναι δυο ειδών, αυτά που είναι προσβάσιμα από τον «έξω κόσμο» (working EFs) και αυτά που είναι μόνο για το λειτουργικό σύστημα (Internal EFs). Κάθε εφαρμογή έχει συνήθως τη δική της DF και μπορεί να χρησιμοποιεί περισσότερα DF για να δομήσει τα δεδομένα της.

Το λειτουργικό των καρτών (OS - Operating System) είναι μια ακολουθία εντολών που όπως αναφέρθηκε νωρίτερα, βρίσκονται μόνιμα εγγεγραμμένες στη ROM. Το OS είναι χτισμένο γύρω από τις εξής λειτουργίες:

1) διαχείριση της επικοινωνίας ανάμεσα στη κάρτα και στο έξω κόσμο κυρίως με την εφαρμογή πρωτοκόλλων,
2) διαχείριση των αρχείων που βρίσκονται στη μνήμη,
3) έλεγχος πρόσβασης στις πληροφορίες και λειτουργίες της κάρτας,
4) εξασφάλιση ασφάλειας με εφαρμογή αλγορίθμων κρυπτογράφησης,
5) παροχή αξιοπιστίας στο σύστημα με την έννοια της συνοχής των δεδομένων, χειρισμό διακοπών (interruptions) και επαναφοράς του συστήματος μετά από σφάλματα.

Ορισμένα διαδεδομένα λειτουργικά είναι το Java Card OS, MULTOS, Windows Card, Cyberflex, MFC, Oscar, StarCOS.

ΚΕΦΑΛΑΙΟ 3^{ο} – ΤΕΡΜΑΤΙΚΟ EFT/POS

3.1 ΤΕΡΜΑΤΙΚΌ EFT/POS - ΟΡΙΣΜΟΙ

Τερματικό EFT/POS ορίζεται η συσκευή που επικοινωνεί με τις κάρτες πληρωμών, τις επεξεργάζεται και μπορεί να υποστηρίζει λειτουργίες πληρωμής, συναλλαγές δηλαδή είτε με μαγνητική ταινία, με επαφή ή και ανέπαφες.

Η φυσική αρχιτεκτονική ενός τέτοιου τερματικού μπορεί να είναι οποιοδήποτε από τις παρακάτω:

- Πλήρως ενσωματωμένο τερματικό: Όλα τα στοιχεία περιλαμβάνονται σε μία μόνο συσκευή.
- Με έξυπνο αναγνώστη: Ο αναγνώστης χειρίζεται το μεγαλύτερο μέρος της επεξεργασίας όσον αφορά τις ανέπαφες συναλλαγές, και απλά διαβιβάζει τα αποτελέσματα με σκοπό την ολοκλήρωση τους στο τερματικό.
- Συνδυασμός τερματικού και αναγνώστη καρτών: Ο αναγνώστης παρέχει επικοινωνία με την κάρτα, ενώ οι πυρήνες και άλλες διαδικασίες βρίσκονται στον τερματικό.

Η δεύτερη και η τρίτη αρχιτεκτονική είναι εφικτές με την προσθήκη ενός ασύρματου αναγνώστη σε ένα απλό υπάρχον τερματικό. Στο υποκεφάλαιο 3.2 θα εστιάσουμε στην δεύτερη εξ αυτών η οποία είναι πολύ διαδεδομένη.

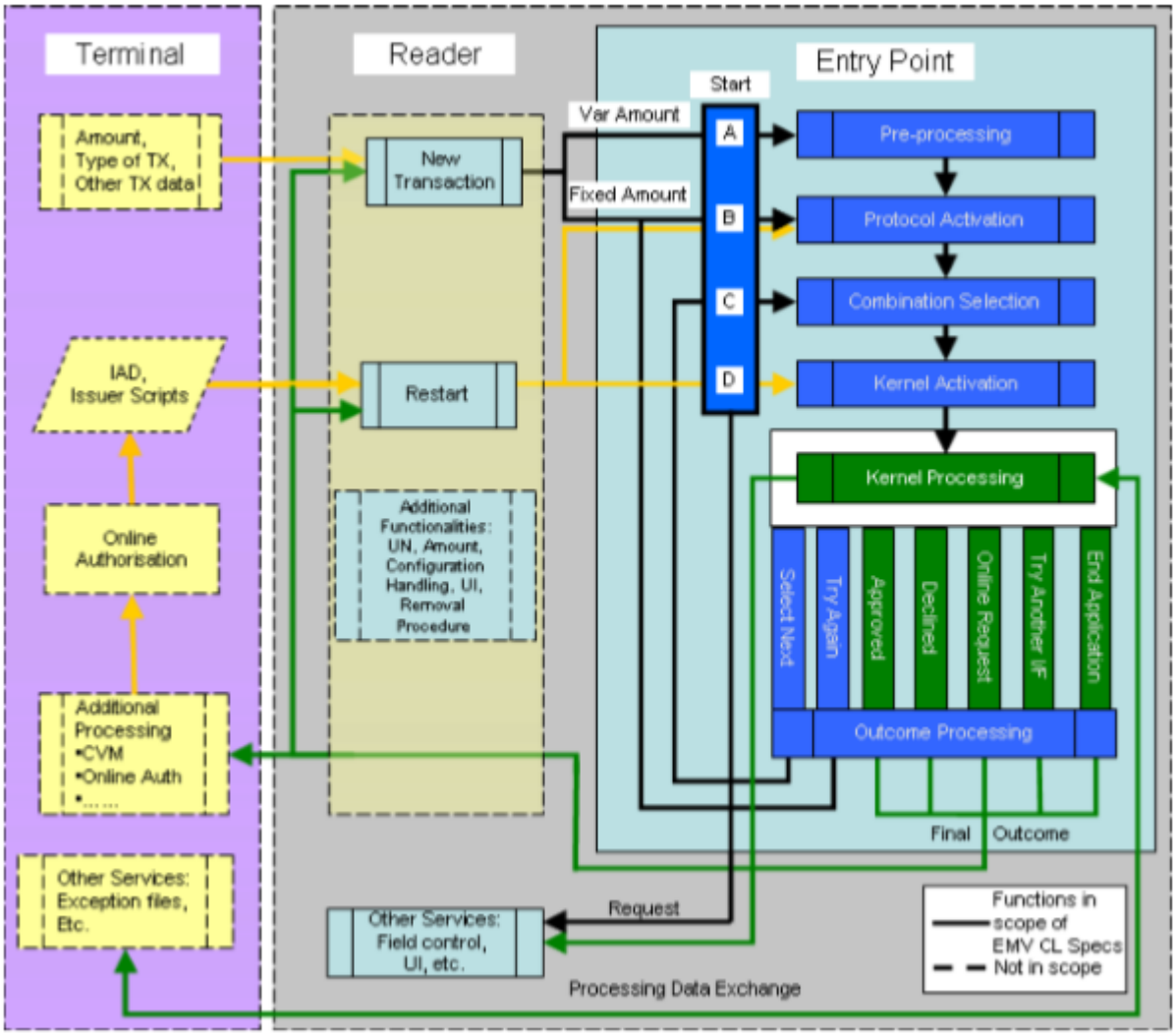
Οι βασικές λειτουργίες του συνολικού συστήματος POS περιλαμβάνουν:

- επικοινωνία με ανέπαφες κάρτες
- επιλογή εφαρμογής και ενεργοποίηση του πυρήνα
- προβολή μηνυμάτων στον κάτοχο της κάρτας
- προβολή μηνυμάτων στον έμπορο
- αποδοχή των στοιχείων της συναλλαγής (πχ ποσό, φιλοδώρημα)
- παροχή online σύνδεσης
- παροχή συλλογής δεδομένων για εκκαθαριστικά

Πριν προχωρήσουμε στις λειτουργίες του συστήματος POS πρέπει πρώτα να δοθεί κάποια επιπλέον ορολογία.

ΣΗΜΕΙΟ ΕΙΣΟΔΟΥ *(Entry Point)*

Το σημείο εισόδου είναι λογισμικό στο σύστημα POS το οποίο είναι υπεύθυνο για την προεπεξεργασία, για την ανίχνευση και επιλογή μιας ανέπαφης εφαρμογής που υποστηρίζεται τόσο από την κάρτα όσο και από τον αναγνώστη, την ενεργοποίηση του κατάλληλου πυρήνα, το χειρισμό των αποτελεσμάτων που επιστρέφει ο πυρήνα.



Σχήμα 3.1: Διάγραμμα λειτουργίας POS. *(Με πράσινο η κίνηση δεδομένων από τον αναγνώστη προς το τερματικό, η αντίστροφη φαίνεται με κίτρινο.)*

ΠΥΡΗΝΑΣ *(Kernel)*

Ένας πυρήνας είναι λογισμικό στο σύστημα POS που επεξεργάζεται ορισμένες ανέπαφες συναλλαγές. Ο πυρήνας επιλέγεται από το σημείο εισόδου με βάση τα χαρακτηριστικά της συναλλαγής, τις εφαρμογές που υποστηρίζονται τόσο από την κάρτα όσο και από τον αναγνώστη και την προτεραιότητα που μπορεί να αποδοθεί σε κάθε εφαρμογή.

ΑΠΟΤΕΛΕΣΜΑ *(Outcome)*

Αποτέλεσμα ονομάζεται η κύρια οδηγία από τον πυρήνα σχετικά με το πώς θα πρέπει να συνεχιστεί η επεξεργασία. Το αποτέλεσμα μαζί με ένα σύνολο παραμέτρων επιτρέπουν στον πυρήνα να υποδείξει την συνέχεια τις ροής εκτέλεσης, όπως για παράδειγμα τα μηνύματα που θα εμφανιστούν ή την ανάγκη επανεκκίνησης μετά από μια ηλεκτρονική εξουσιοδότηση.

Όταν ένας πυρήνας παρέχει ένα αποτέλεσμα, τον έλεγχο αναλαμβάνει πίσω το Σημείο Εισόδου το οποίο χειρίζεται κάποιες παραμέτρους και στη συνέχεια επεξεργάζεται το αποτέλεσμα ή το διαβιβάζει στον αναγνώστη ως τελικό αποτέλεσμα.

Σε περίπτωση που το Σημείο Εισόδου δεν είναι σε θέση να επιλέξει έναν κατάλληλο πυρήνα τότε παράγει τελικό αποτέλεσμα και μεταβιβάζει τον έλεγχο πίσω στον αναγνώστη.

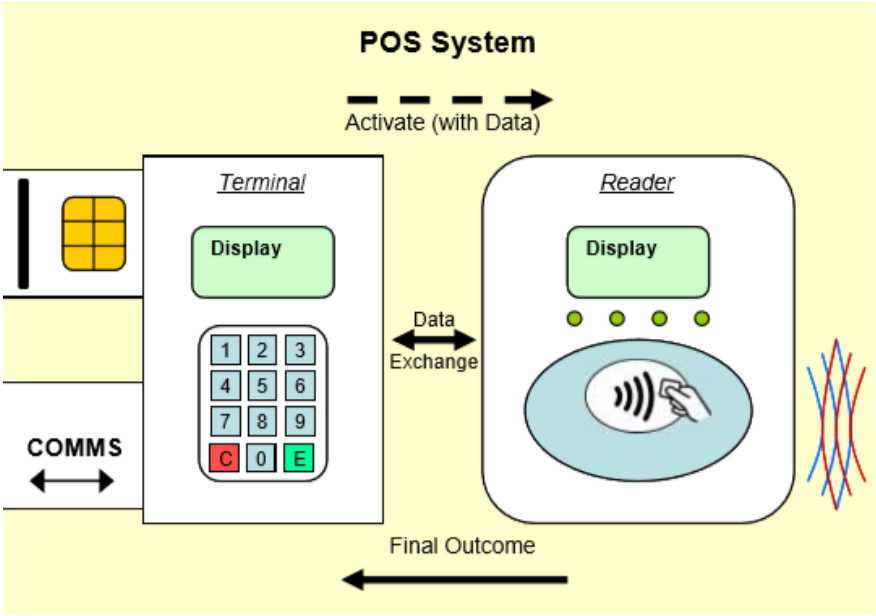
Στο σχήμα 3.1 φαίνεται και το λογικό διάγραμμα λειτουργίας του συστήματος POS και τα στοιχεία που το αποτελούν όπως αυτά προαναφέρθηκαν.

3.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΕΡΜΑΤΙΚΟΎ EFT/POS

Στο παρόν υποκεφάλαιο, θα εξεταστεί η πιο διαδεδομένη αρχιτεκτονική ενός τερματικού συστήματος EFT/POS.

Το δεξιό τμήμα του σχήματος 3.2 φαίνεται ο ασύρματος αναγνώστης ο οποίος επικοινωνεί με την ανέπαφη κάρτα και επεξεργάζεται την εφαρμογή. Συνεπώς, αυτός περιλαμβάνει τη λειτουργικότητα του Σημείου Εισόδου και των πυρήνων. Περιλαμβάνει επίσης τη διεπαφή του πελάτη, η οποία μπορεί να αποτελείται από οθόνη όπου βλέπει ο κάτοχος της κάρτας, αλλά και τους άλλα οπτικοακουστικά μέσα κατάστασης φώτα led μικρό ηχείο.

Στο αριστερό τμήμα του σχήματος φαίνεται ένα κλασσικό τερματικό επαφής και περιλαμβάνει την είσοδο και την οθόνη του εμπόρου, τις θύρες για την online σύνδεση, καθώς και οποιεσδήποτε εναλλακτικές διεπαφές της κάρτας με μαγνητική λωρίδα ή επαφή. [11]



Σχήμα 3.2: Σύστημα POS

3.3 ΕΥΘΥΝΕΣ ΤΟΥ ΤΕΡΜΑΤΙΚΟΥ EFT/POS ΚΑΙ ΤΟΥ ΑΝΑΓΝΩΣΤΗ

Στην περίπτωση που το σύστημα POS έχει διακριτό αναγνώστη και το τερματικό, αυτά εκτελούν διαφορετικές λειτουργίες. Ξεκινώντας από τον αναγνώστη:

Είναι υπεύθυνος για την ασύρματη επικοινωνία με τις κάρτες, την επιλογή εφαρμογών και την ενεργοποίηση του κατάλληλου πυρήνα, την εκτέλεση των εφαρμογών πυρήνα, την επιλογή CVM, τη δημιουργία τελικού αποτελέσματος και του συνόλου παραμέτρων που το συνοδεύουν. Ακόμα διαχειρίζεται διακοπές-timeouts (που προκύπτουν για παράδειγμα στην περίπτωση πρόωρης απομάκρυνσης της κάρτας) και τη διαχείριση του ηλεκτρομαγνητικού πεδίου (ενεργοποίηση / απενεργοποίηση).

Το τερματικό από την άλλη είναι αρμόδιο για την παροχή δεδομένων από τον έμπορο, την επεξεργασία των τελικών αποτελεσμάτων όπως προκύπτουν από τον αναγνώστη, συμπεριλαμβανομένου του χειρισμού των αιτήσεων αυθεντικοποίησης και των απαντήσεων τους. Επίσης επαληθεύει τον κάτοχο της κάρτας (εκτός εάν αυτό γίνει σε άλλο περιβάλλον όπως το κινητό τηλέφωνο), διαχειρίζεται τα μηνύματα εξουσιοδότησης και τις μη ανέπαφες συναλλαγές (επαφή και μαγνητική λωρίδα). Τέλος είναι υπεύθυνο για τον χειρισμό άλλον πτυχών της επεξεργασίας όπως timeouts και ακυρώσεις συναλλαγών.

Ανάλογα με το σχεδιασμό ορισμένες λειτουργίες μπορεί να είναι υπό την ευθύνη είτε του τερματικού είτε του αναγνώστη. Τέτοιες λειτουργιές συχνά έχουν να κάνουν με την έναρξη

νέων συναλλαγών, συμπεριλαμβανομένης της αφαίρεσης καρτών και της κατάστασης πεδίου επαφής μεταξύ συναλλαγών ή την εμφάνιση μηνυμάτων στον έμπορο.

Γενικότερα πάντως όσον αφορά τον χρονισμό, ο αναγνώστης κυρίως διαχειρίζεται θέματα χρονισμού της κάρτας εντός του πεδίου ενώ το τερματικό θέματα χρονισμού τις γενικότερης συναλλαγής και της online σύνδεσης.

3.4 ΛΕΙΤΟΥΡΓΙΕΣ ΣΥΣΤΗΜΑΤΟΣ POS

Οι λειτουργίες ενός συστήματος POS, όπως περιγράφηκαν στο υποκεφάλαιο 3.3, είναι πολλές, στα παρακάτω θα περιγραφούν οι βασικότερες αυτών που αφορούν φυσικά σε ανέπαφες κάρτες.

Αποφυγή παρεμβολής ταυτόχρονων συναλλαγών από διαφορετικές επαφές

Σε ένα POS σύστημα ικανό να δέχεται συναλλαγές μέσω πολλαπλών διεπαφών, όλες οι επιτρεπόμενες διεπαφές πρέπει να τίθενται στη διάθεση του εμπόρου/κατόχου της κάρτας για την πραγματοποίηση μιας συναλλαγής. Ωστόσο εάν ο κάτοχος της κάρτας επιλέξει τη συναλλαγή με επαφή, για να αποφευχθεί η ενδεχόμενη ασύρματη ζεύξη, το σύστημα POS πρέπει να απενεργοποιήσει την ανέπαφη διεπαφή πριν ξεκινήσει την συναλλαγή και να την κρατήσει απενεργοποιημένη για όλη τη διάρκεια της συναλλαγής.

Αποφυγή επικαλυπτόμενων συναλλαγών

Το σύστημα POS θα πρέπει να διασφαλίζει ότι μια νέα συναλλαγή δεν θα ξεκινάει μέχρι την ολοκλήρωση της προηγούμενης συναλλαγής. Η ολοκλήρωση μιας συναλλαγής συνίσταται από την κατάσταση ολοκλήρωσης της συναλλαγής του POS και την απομάκρυνση της κάρτας.

Σε ορισμένες εφαρμογές για την ολοκλήρωση της συναλλαγής μπορεί να αρκεί η επιβεβαίωση ενός μόνο από τα παραπάνω. Για παράδειγμα σε ένα μηχάνημα αυτόματης πώλησης όπου ο επόμενος πελάτης δεν πρόκειται να ξεκινήσει μια συναλλαγή πριν την απομάκρυνση του πρώτου, η λογική για την τερματισμό της τελευταίας συναλλαγής και την αρχή της επόμενης είναι αρκετά απλή. Αντίθετα σε εφαρμογές πληρωμής κατά την είσοδο, μπορεί να είναι απαραίτητο το POS να ελέγξει την απομάκρυνση της πρώτης κάρτας και να εξασφαλίσει κατάλληλο χρονικό διάστημα μέχρι την εκκίνηση της επόμενης συναλλαγής.

Δυνατότητα ακύρωσης συναλλαγής

Σημαντική είναι και η δυνατότητα ακύρωσης μίας συναλλαγής σε περίπτωση που ο κάτοχος της κάρτας δεν επιδείξει την κάρτα σε ένα εύλογο χρονικό διάστημα. Το σύστημα POS μπορεί

να προσπαθήσει να ολοκληρώσει τη συναλλαγή χρησιμοποιώντας κάποια άλλη διεπαφή, είτε να τερματίσει τη συναλλαγή.

Διαχείριση πεδίου

Το εάν το πεδίο είναι ενεργοποιημένο ή απενεργοποιημένο μεταξύ των συναλλαγών θα εξαρτηθεί από το περιβάλλον λειτουργίας και το σύστημα POS είναι υπεύθυνο για τη διασφάλιση της κατάστασης του πεδίου.

Εμφάνιση ποσού

Σε περιβάλλοντα όπου ο τύπος συναλλαγής και το ακριβές ποσό είναι γνωστά πριν την εκκίνηση, το ποσό πρέπει να αναγράφεται στον κάτοχο της κάρτας, κατά προτίμηση μέσω οθόνης. Σε ορισμένες περιπτώσεις, το ποσό μπορεί να εμφανίζεται σε ετικέτες, όπως οι αναγραφόμενες τιμές σε μηχάνημα αυτόματης πώλησης. Σε τέτοιες περιπτώσεις τα ποσά γνωστοποιούνται στον αναγνώστη καθώς ξεκινά η συναλλαγή. Ενώ σε άλλα περιβάλλοντα ενδέχεται να μην γνωρίζει τον τύπο συναλλαγής ή το ποσό μέχρι να ολοκληρωθεί η αλληλεπίδραση με την κάρτα.

Αποδείξεις συναλλαγής

Το σύστημα POS μπορεί να έχει κανόνες αποδοχής σχετικά με τα έσοδα, ειδικά για την τοποθεσία, το περιβάλλον και ενδεχομένως το σύστημα πληρωμών.

3.5 ΡΥΘΜΙΣΕΙΣ ΣΥΣΤΗΜΑΤΟΣ POS

Συνεχίζουμε κάνοντας αναφορά στις βασικές ρυθμίσεις του συστήματος, οι οποίες είναι απαραίτητες για την ορθή λειτουργία του. Πιο συγκεκριμένα το σύστημα θα πρέπει να παρέχει επιλογές που θα καθορίζουν:

Κωδικό χώρας και νομίσματος

Το σύστημα POS πρέπει να ρυθμίζεται με έναν κωδικό χώρας (ετικέτα '9F1A') και με έναν ή περισσότερους κωδικούς νομίσματος συναλλαγών (ετικέτα '5F2A'), ανάλογα με το αν υποστηρίζονται πολλαπλά νομίσματα.

Τρόπο εκκίνησης μιας συναλλαγής

Το σύστημα POS πρέπει να είναι ρυθμίζεται έτσι ώστε μια συναλλαγή είτε να ξεκινά με εντολή τερματικού είτε να αυτόματα μετά την ολοκλήρωση της προηγούμενης συναλλαγής.

Αυτή η ρύθμιση γίνεται με την χρήση παραμέτρου Autorun και επιλογές όχι / ναι.

Εάν η τιμή του Autorun είναι "Όχι", τότε η έναρξη της συναλλαγής ξεκινάει από τον έμπορο, συνήθως εισάγοντας το ποσό. Εάν η τιμή του Autorun είναι "Ναι", τότε η έναρξη της

συναλλαγής πραγματοποιείται όταν μια κάρτα εισέρχεται στο πεδίο και απαντά, υποδεικνύοντας την παρουσία της.

Υποστηριζόμενους τρόπους λειτουργίας

Οι τρόποι λειτουργίας που υποστηρίζονται από ένα σύστημα POS εξαρτώνται από το περιβάλλον και τους κανόνες αποδοχής. Οι πυρήνες πρέπει να διαθέτουν τη συγκεκριμένη πληροφορία για να ζητήσουν τα απαραίτητα στοιχεία και να εκτελέσουν την προβλεπόμενη ροή επεξεργασίας. Επομένως, οι ρυθμίσεις υποδεικνύουν τους τρόπους λειτουργίας που υποστηρίζονται και παρέχονται στον πυρήνα. Αυτοί είναι: Λειτουργία EMV, Λειτουργία μαγνητικής λωρίδας, ταυτόχρονη υποστήριξη και των δύο προηγούμενων λειτουργιών

Τύπους υποστηριζόμενων συναλλαγών

Το σύστημα POS πρέπει να γνωρίζει τους τύπους συναλλαγών που υποστηρίζει, οι οποίοι και είναι: Αγορά, Αγορά με επιστροφή χρημάτων, Προκαταβολή μετρητών (επιστροφή μετρητών), Επιστροφή χρημάτων.

Ρυθμίσεις Πυρήνα και Σημείου Εισόδου

Για κάθε υποστηριζόμενο συνδυασμό Εφαρμογής – Πυρήνα {Application ID - Kernel ID}, ο αναγνώστης έχει:

1. Ρυθμίσεις πυρήνα - Για κάθε υποστηριζόμενο τύπο συναλλαγής αντιστοιχεί ένα σύνολο στατικών δεδομένων για τη ρύθμιση του πυρήνα.

Η τιμή αυτών των δεδομένων διατηρείται από τη μια συναλλαγή στην άλλη και αντιπροσωπεύει πληροφορίες που περιγράφουν, τη λειτουργία (EMV / mag-stripe), την υποστήριξη CVM, τη λειτουργία online / offline και το σύνολο δεδομένων δημόσιου κλειδιού. Οι ενημερώσεις των τιμών πραγματοποιούνται σε εξαιρετικές περιπτώσεις και συμβαίνουν πάντα εκτός της επεξεργασίας συναλλαγών. Ορισμένες τιμές μπορούν να έχουν διαφορετικές σημασίες για διαφορετικούς πυρήνες.

2. Ρυθμίσεις σημείου εισόδου - Για κάθε υποστηριζόμενο τύπο συναλλαγής αντιστοιχεί ένα σύνολο στατικών δεδομένων για επεξεργασία από το σημείου εισόδου.

Τα δεδομένα αυτά αντιπροσωπεύουν τις ρυθμίσεις συναλλαγών, όπως τα όρια των ανέπαφων συναλλαγών και τα όρια CVM. Ενημερώσεις πραγματοποιούνται και σε αυτή την περίπτωση εκτός της επεξεργασίας συναλλαγών.

ΚΕΦΑΛΑΙΟ 4ο - ΤΕΧΝΟΛΟΓΙΑ NFC

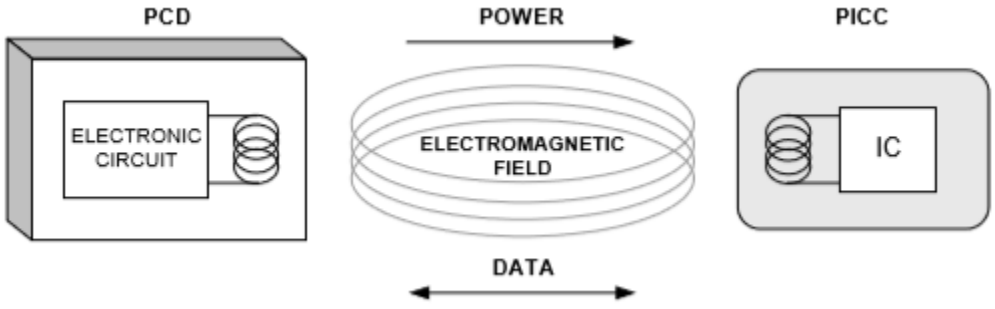
4.1 CONTACTLESS ΣΥΣΤΗΜΑ

Τα βασικά στοιχεία ενός ανέπαφου συστήματος είναι ο ανέπαφος αναγνώστης ή αλλιώς Proximity Coupling Device (PCD) και ένας αναμεταδότης ή αλλιώς Proximity IC Card (PICC).

Στο παρόν κεφάλαιο, θα αναφερόμαστε στο τερματικό EFT/POS ως PCD και στην κάρτα που υποστηρίζει ανέπαφες συναλλαγές ως PICC.

Το PCD είναι μια κεραία συνδεδεμένη σε ένα ηλεκτρονικό κύκλωμα. Το PICC αποτελείται από μια επαγωγική κεραία και ένα ολοκληρωμένο κύκλωμα συνδεδεμένο στα άκρα της κεραίας. Ο συνδυασμός PCD-PICC συμπεριφέρεται σαν μετασχηματιστής. Ένα εναλλασσόμενο ρεύμα διέρχεται από ένα πρωτεύον πηνίο (PCD κεραία) και δημιουργεί ένα ηλεκτρομαγνητικό πεδίο, το οποίο προκαλεί ρεύμα στο δευτερεύον πηνίο (κεραία PICC). Το PICC μετατρέπει το ηλεκτρομαγνητικό πεδίο (ή το πεδίο RF) που μεταδίδεται από το PCD σε τάση συνεχούς ρεύματος μέσω ανόρθωσης και χρησιμοποιεί την τάση DC για την τροφοδοσία των εσωτερικών κυκλωμάτων του PICC. Η διαμόρφωση και ο συντονισμός και των δύο κεραιών καθορίζουν την απόδοση ζεύξης από τη μια συσκευή στην άλλη.

Η προσθήκη πληροφοριών σε ένα φέρον σήμα ονομάζεται διαμόρφωση. Ένα φέρον σήμα χαρακτηρίζεται από το εύρος, τη φάση και τη συχνότητά του. Επομένως, μπορούν να προστεθούν πληροφορίες στο φέρον σήμα με την αλλαγή ενός ή περισσοτέρων από αυτά τα χαρακτηριστικά. Οι μέθοδοι διαμόρφωσης που χρησιμοποιούνται στις περιπτώσεις καρτών RFID και NFC, χωρίζονται στη διαμόρφωση πλάτους όπου το επίπεδο του φέροντος σήματος μεταβάλλεται με την πάροδο του χρόνου και στη διαμόρφωση φάσης όπου το φέρον σήμα είτε προπορεύεται είτε καθυστερεί προσωρινά, αλλάζοντας τη φάση του.



Σχήμα 4.1: Απεικόνιση της ασύρματης επικοινωνίας PCD και PICC

Η ενέργεια RF που μεταδίδεται από το PCD και λαμβάνεται από το PICC όχι μόνο το τροφοδοτεί, αλλά χρησιμοποιείται επίσης για τη μεταφορά των δεδομένων μέσω της διαμόρφωσης του φορέα. Το PICC αποκωδικοποιεί και επεξεργάζεται τα δεδομένα και απαντάει πίσω στο PCD μέσω διαμόρφωσης φορτίου.
Η διαμόρφωση φορτίου βασίζεται στην ηλεκτρομαγνητική σύζευξη (δηλαδή την αμοιβαία επαγωγή) μεταξύ PICC και PCD παρόμοια με τη μεταφορά ισχύος και την επικοινωνία από PCD σε PICC. Το PICC αλλάζει το ρεύμα στην κεραία του και αυτή η διακύμανση ανιχνεύεται από το PCD ως μικρή αλλαγή στο ρεύμα της δικής του κεραίας.

4.2 NFC ΤΕΧΝΟΛΟΓΙΑ (ISO 14443 – 2 –A -B)

Η τεχνολογία Near Field Communication (NFC) είναι μια τεχνολογία ασύρματης συνδεσιμότητας μικρής εμβέλειας, η οποία χρησιμοποιεί επαγωγή μαγνητικού πεδίου για την επικοινωνία μεταξύ ηλεκτρονικών συσκευών σε κοντινή απόσταση.

Με βάση την τεχνολογία RFID, το NFC παρέχει ένα μέσο για τα πρωτόκολλα ταυτοποίησης που επικυρώνουν την ασφαλή μεταφορά δεδομένων. Το NFC επιτρέπει στους χρήστες να πραγματοποιούν ανέπαφες συναλλαγές, να έχουν πρόσβαση σε ψηφιακό περιεχόμενο και να συνδέουν ηλεκτρονικές συσκευές απλά πλησιάζοντας αυτές σε κοντινή απόσταση υπό την προϋπόθεση πως υποστηρίζουν τη συγκεκριμένη τεχνολογία συνδεσιμότητας.

Μια NFC συσκευή μπορεί να βρίσκεται σε 3 διαφορετικές καταστάσεις λειτουργίας (modes). Η πρώτη είναι η Read/Write όπου η συσκευή είναι Active και μπορεί να διαβάσει ή να γράψει το περιεχόμενο μίας ετικέτας. Η δεύτερη είναι η Card emulation όπου επιτρέπει τις NFC συσκευές να συμπεριφέρονται σαν έξυπνη κάρτα. Και τέλος η τελευταία είναι η Peer to Peer όπου επιτρέπει σε δύο συσκευές να επικοινωνήσουν μεταξύ τους παρόμοια όπως με τεχνολογίες τύπου Bluetooth ή WiFi.

Δύο πρότυπα ISO έχουν καθιερωθεί όσον αφορά τις RFID υψηλές συχνότητες. Συγκεκριμένα, πρόκειται για τα ISO14443 και ISO15693.

Η χρήση των προτύπων ISO, παρέχει μια βάση στην οποία οι κατασκευαστές πομποδεκτών αλλά και καρτών/ετικετών μπορούν να βασίζονται και να ακολουθούν με σκοπό τη διασφάλιση της διαλειτουργικότητας. Παρέχει ένα πλαίσιο για μελλοντικές βελτιώσεις/προσθήκες αλλά και τη βάση για άλλους φορείς προδιαγραφών.

Το πρότυπο ISO / IEC 14443 χρησιμοποιείται κυρίως για εφαρμογές προσέγγισης/απόστασης όπως οι ανέπαφες πληρωμές, ο έλεγχος πρόσβασης υψηλής ασφάλειας, τα ePassports κ.λπ. Το

ISO14443 χωρίζεται σε τέσσερα (4) μέρη για δύο τύπους PICC που ονομάζονται Type A και Type B:

- ISO14443-1: Φυσικά χαρακτηριστικά καρτών (PICC)
- ISO14443-2: Διασύνδεση ισχύος και σήματος
- ISO14443-3: Initialization (Activation) and Anti-Collision Command Set Protocol
- ISO14443-4: Πρωτόκολλο μετάδοσης (framework)

    - Χρησιμοποιεί το ISO7816-4 για το σετ εντολών του επιπέδου εφαρμογής

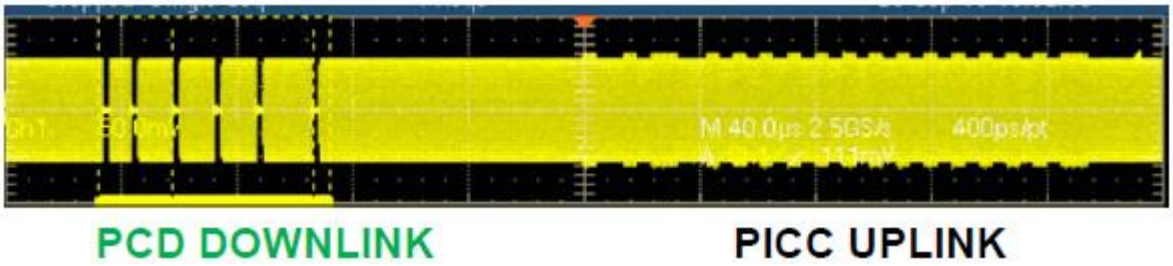
Παρακάτω θα οριστεί η φυσική διεπαφή μεταξύ του PCD και του PICC. Γενικά, η ετικέτα PICC (τύπου A και τύπου B) είναι παθητική - δεν έχει πηγή ισχύος και αντλεί όλη της την ενέργεια από το σήμα μετάδοσης του αναγνώστη PCD. Η επικοινωνία βασίζεται στην επαγωγική σύζευξη μεταξύ ενεργού αναγνώστη και παθητικής ετικέτας. Θα αναφερθούμε στο κανάλι του PCD στο PICC ως το downlink κανάλι ζεύξης και το κανάλι από το PICC στο PCD ως το uplink κανάλι ζεύξης. Σύμφωνα με το πρότυπο, η συχνότητα φορέα του αναγνώστη PCD είναι fc = 13,56MHz.

4.2.1 TYPE A

Θα αναφερθούμε εκτενέστερα στο συγκεκριμένο τύπο καθώς τέτοιες κάρτες χρησιμοποιήθηκαν στο πειραματικό μας μέρος, περισσότερες λεπτομέρειες δίνονται στο Κεφάλαιο 6.

Διαμόρφωση Downlink: Η επικοινωνία από τον αναγνώστη PCD στην ετικέτα PICC χρησιμοποιεί Amplitude Shift Keying (ASK) με βάθος διαμόρφωσης 100%. Τα bits τα οποία μεταδίδονται, κωδικοποιούνται με τη χρήση του σχήματος modified Miller, όπου όταν μεταδίδεται ‘0’ δεν προκαλείται καμία μεταβολή εκτός και αν αυτό ακολουθείται από ‘0’. Προκειμένου να εξασφαλιστεί η συνεχής τροφοδοσία ισχύος στην παθητική ετικέτα, το μήκος των διαστημάτων όπου το διαμορφωμένο σήμα έχει μηδενικό πλάτος δεν ξεπερνούν τα 2-3μs.

Διαμόρφωση Uplink: Δεδομένου ότι το PICC δεν έχει ανεξάρτητη πηγή ισχύος, μεταδίδει το σήμα του μέσω διαμόρφωσης φορτίου ενός υπο-φορέα σε συχνότητα fsc = fc / 16 ≈ 847kHz. Τα bits που μεταδίδονται είναι κωδικοποιημένα με τη μέθοδο Manchester.



Σχήμα 4.2: Επικοινωνία PCD σε PICC και PICC σε PCD

Η επικοινωνία ξεκινάει στα 106kbps και μπορεί να αυξηθεί στα 212kbps, 424kbps ή στα 848kbps, εάν υποστηρίζεται και από το PCD αλλά και το PICC.

ISO14443 -3 TYPE A COMMAND SET

Μία τυπική επικοινωνία μεταξύ PCD και PICC περιλαμβάνει εντολές από την πλευρά του PCD και απαντήσεις από την πλευρά του PICC. Παρακάτω περιγράφονται οι σημαντικότερες.

REQA & WUPA

Μέσω αυτών των εντολών, το PCD δειγματοληπτεί το πεδίο για διαθέσιμες κάρτες PICC μέσα σε αυτό και αναμένει την απάντηση ATQA.

ANTICOLLISION

Πρόκειται για την εντολή η οποία χρησιμοποιείται ώστε το PCD να λάβει το UID του PICC και να μπορεί να ανιχνεύσει την παρουσία περισσότερων από μίας (1) κάρτας. Η απάντηση στη συγκεκριμένη εντολή, είναι το UID της κάρτας PICC. Τα UIDs των τύπου A PICCs αποτελούνται από 4, 7 ή 10 bytes. Το μέγεθος της απάντησης είναι πάντα 5 bytes. Στο τέλος κάθε απάντησης βρίσκεται το BCC το οποίο είναι ένα byte επαλήθευσης. Επομένως, για κάρτες με μήκος UID=4 bytes επαρκεί ένα ζευγάρι εντολής απάντησης ANTICOLLISION για να περιγράψει το UID. Αντίστοιχα, για UID=7 bytes, απαιτούνται δύο ζευγάρια. Τέλος, για 10 bytes, χρειάζονται τρία ζευγάρια.

SEL	UID Size	Response (UID CLn)
'93'	4	UID CL1: uid_0 uid_1 uid_2 uid_3 BCC
'93'	> 4	UID CL1: CT uid_0 uid_1 uid_2 BCC
'95'	7	UID CL2: uid_3 uid_4 uid_5 uid_6 BCC
'95'	> 7	UID CL2: CT uid_3 uid_4 uid_5 BCC
'97'	10	UID CL3: uid_6 uid_7 uid_8 uid_9 BCC

Σχήμα 4.3: Απάντηση σε ANTICOLLISION

SELECT

Είναι η εντολή με την οποία το PCD επιλέγει ένα PICC με τη χρήση του UID του. Η απάντηση στην εντολή SELECT είναι η SAK (Select Acknowledge).

HLTA

Η εντολή HLTA χρησιμοποιείται για τη διακοπή της επικοινωνίας με το PICC ενώ εξακολουθεί να βρίσκεται στο πεδίο του PCD. Η εντολή WUPA χρησιμοποιείται μετά από μία HALTA.

4.2.2 TYPE B

Οι κάρτες τύπου PICC τύπου B χρησιμοποιήθηκαν αρκετά αργότερα από τις τύπου A, και παρουσιάζουν αρκετά πλεονεκτήματα. Για παράδειγμα, παρουσιάζει υψηλότερο ρυθμό μετάδοσης πληροφορίας ο οποίος μπορεί να προσαρμοστεί ανάλογα με τις απαιτήσεις της εφαρμογής. Επίσης, ο μηχανισμός ANTICOLLISION είναι αποδοτικότερος σε σχέση με τον πρώτο τύπο.

Διαμόρφωση Downlink: Χρησιμοποιείται Amplitude Shift Key (ASK) με βάθος διαμόρφωσης 10% για την επικοινωνία του PCD προς το PICC. Τα bits τα οποία μεταδίδονται, κωδικοποιούνται με κωδικοποίηση NRZ.

Διαμόρφωση Uplink: Η επικοινωνία από το PICC στο PCD χρησιμοποιεί διαμόρφωση φορτίου σε συχνότητα υπο-φορέα 848kHz. Ο υπο-φορέας είναι διαμορφωμένος σε BPSK.

Η επικοινωνία ξεκινάει στα 106kbps και μπορεί να αυξηθεί στα 212kbps, 424kbps ή στα 848kbps, εάν υποστηρίζεται και από το PCD αλλά και το PICC.

ISO14443 -3 TYPE B COMMAND SET

Όντας περισσότερο αποτελεσματικό από το πρότυπο ISO14443A, μόνο τέσσερες (4) από τις αρχικές εντολές χρησιμοποιούνται για την επικοινωνία.

REQB & WUPB

Οι εντολές REQB και WUPB στέλνονται από το PCD και χρησιμοποιούνται για να ανιχνεύσουν στο πεδίο πιθανά PICC τύπου B. Η εντολή WUPB χρησιμοποιείται επίσης για να ενεργοποιήσει τα PICCs που βρίσκονται σε κατάσταση idle (HALT). Η εντολή που χρησιμοποιείται ως απάντηση, ονομάζεται ATQB.

ATTRIB

Η εντολή ATTRIB, η οποία αποστέλλεται από το PCD περιλαμβάνει πληροφορίες που απαιτούνται για την επιλογή ενός συγκεκριμένου PICC. Το PICC λαμβάνει τη συγκεκριμένη ATTRIB εντολή με το αναγνωριστικό της και τότε εγγράφεται σε ένα συγκεκριμένο κανάλι και απαντά μόνο σε εντολές που περιλαμβάνουν το μοναδικό CID (Card Identifier).

HLTB

Η εντολή HLTB χρησιμοποιείται για να θέσει το PICC σε κατάσταση HALT και να σταματήσει να απαντά στην εντολή REQB. Αφού απαντήσει στην εντολή HLTB, το PICC πρέπει να αγνοήσει οποιαδήποτε εντολή εκτός της WUPB.[20]

4.3 ΕΠΙΘΕΣΕΙΣ ΣΕ ΣΥΣΤΗΜΑΤΑ ΑΝΕΠΑΦΩΝ ΣΥΝΑΛΛΑΓΩΝ

Όπως ήδη έχει αναφερθεί, οι ασύρματες τεχνολογίες έχουν διευκολύνει ιδιαίτερα τις οικονομικές μας συναλλαγές. Φυσικά, δεν πρέπει να παραβλέπουμε τους κινδύνους που έχουν προκύψει από τη χρήση αυτών, σε σχέση πάντοτε και με τις ενσύρματες τεχνολογίες.

Eavesdropping

Μέσω της επίθεσης τύπου Eavesdropping, ο επιτιθέμενος μπορεί δυνητικά να συλλέξει σήματα που εκπέμπονται κατά τη διάρκεια των ανέπαφων συναλλαγών. Ο υποκλοπέας παρακολουθεί την μετάδοση των δεδομένων χρησιμοποιώντας βασικό εξοπλισμό, όπως μια κεραία, ενώ πραγματοποιείται μια νόμιμη συναλλαγή. Οι πληροφορίες που συλλέγονται κατά τη διάρκεια αυτής της επίθεσης θα μπορούσαν να έχουν σοβαρές συνέπειες για τον ιδιοκτήτη της κάρτας και τις τράπεζες με τις οποίες συσχετίζεται. Τα δεδομένα που συλλέγονται από την υποκλοπή μπορούν να αποθηκευτούν για περαιτέρω ανάλυση και να χρησιμοποιηθούν μελλοντικά για την κλωνοποίηση ετικετών. Ο συγκεκριμένος τύπος επίθεσης δοκιμάστηκε πειραματικά και αναλύεται σε επόμενο κεφάλαιο.

Jamming

Η επίθεση τύπου jamming καθιστά το κανάλι επικοινωνίας μεταξύ PCD και PICC ακατάλληλο κι αυτός είναι ο λόγος που εντάσσεται στην κατηγορία Άρνησης Υπηρεσιών (DoS). Οι επιθέσεις τύπου Jamming αναφέρονται στην σκόπιμη διατάραξη της ασύρματης ζεύξης μεταξύ μιας ετικέτας και ενός αναγνώστη. Η επίθεση αφορά στην επικοινωνία μεταξύ των δύο συσκευών και μπορεί να πραγματοποιηθεί χρησιμοποιώντας ισχυρούς πομπούς που παραλύουν την επικοινωνία της ετικέτας και παράγουν ένα θόρυβο ίσης συχνότητας με το σύστημα που χρησιμοποιείται και μεγαλύτερου πλάτους (έντασης).

Wireless Copying

Οι επιθέσεις τύπου Wireless Copying είναι η πιο πρόσφατη εξέλιξη όσον αφορά την ασφάλεια των ανέπαφων τραπεζικών καρτών. Ο επιτιθέμενος με μία τροποποιημένη έξυπνη συσκευή είναι σε θέση να συλλέξει προσωπικά δεδομένα εάν βρίσκεται σε πολύ μικρή απόσταση από το θύμα. Οι λεπτομέρειες που λαμβάνονται είναι το όνομα του κάτοχου του λογαριασμού, η ημερομηνία λήξης του αριθμού λογαριασμού καθώς και οι τελευταίες συναλλαγές. Για την πραγματοποίηση αυτής της επίθεσης, απαιτείται μία έξυπνη συσκευή που να υποστηρίζει τεχνολογία NFC καθώς και η εγκατάσταση κάποιας σχετικής εφαρμογής (υπάρχουν αρκετές διαθέσιμες εφαρμογές στο Google Play store, κ.α.). Με την τοποθέτηση της έξυπνης συσκευής σε μικρή απόσταση από την κάρτα του θύματος, ο επιτιθέμενος μπορεί να ανακτήσει τα δεδομένα χωρίς το θύμα να αντιληφθεί πως είναι στόχος επίθεσης. [13]

Όπως προκύπτει λοιπόν, το NFC από μόνο του δεν μπορεί να εγγυηθεί για την ασφαλή επικοινωνία. Οι εφαρμογές θα πρέπει να χρησιμοποιούν υψηλότερου επιπέδου πρωτόκολλο κρυπτογράφησης για να εδραιώσουν ένα ασφαλές κανάλι.

ΚΕΦΑΛΑΙΟ 5^{ο} - ΑΣΦΑΛΕΙΑ EMV MODE

5.1 ΣΥΝΑΛΛΑΓΗ

Κατά την εκτέλεση μιας συναλλαγής, το chip επεξεργάζεται πληροφορίες και καθορίζει πολλούς από τους κανόνες οι οποίοι θα παίξουν ρόλο στο τελικό αποτέλεσμα. Το τερματικό EFT/POS βοηθά στο να εφαρμοστούν οι συγκεκριμένοι κανόνες που έχουν τεθεί από τον εκδότη της κάρτας στο chip. Τέτοιου είδους υπηρεσίες είναι, η offline αυθεντικοποίηση δεδομένων, η επαλήθευση του κατόχου της κάρτας μέσω χρήσης κωδικού PIN ή υπογραφής, online authorization, κ.λπ. Η Τράπεζα θα καθορίσει ποιες από τις υπηρεσίες απαιτούνται για την εκάστοτε τρέχουσα συναλλαγή, μέσων των κανόνων που έχουν οριστεί στο chip.

Αρχικά, το τερματικό και το chip βρίσκουν τις εφαρμογές που υποστηρίζονται και από τα δύο και επιλέγουν ποια θα χρησιμοποιηθεί τελικά για τη διεξαγωγή της συναλλαγής. Το τερματικό EFT/POS διαβάζει τις απαραίτητες πληροφορίες από το chip. Ύστερα, πραγματοποιείται το Offline Data Authentication και επιλέγεται η μέθοδος αυθεντικοποίησης (Static Data Authentication, Dynamic Data Authentication, ή Combined Data Authentication). Πραγματοποιούνται έλεγχοι ώστε να επιβεβαιωθεί πως το chip επιτρέπεται να πραγματοποιήσει τη συναλλαγή. Ο κάτοχος της κάρτας επαληθεύεται μέσω κάποιας μεθόδου που να υποστηρίζεται από το τερματικό EFT/POS και να έχει συμφωνηθεί με το chip. Τέτοιες μεθόδους αποτελούν η υπογραφή, online PIN, offline κρυπτογραφημένο PIN, offline plaintext PIN είτε χωρίς CVM (No Cardholder Verification Method). Το τερματικό EFT/POS πραγματοποιεί πληθώρα ελέγχων, όπως το floor limit ώστε να εξακριβωθεί εάν απαιτείται να γίνει online η επεξεργασία της συναλλαγής. Αφού πραγματοποιηθεί ανάλυση των αποτελεσμάτων από τις προηγούμενες φάσεις, η εφαρμογή του τερματικού EFT/POS ζητά το αποτέλεσμα (decline offline, approve offline, go online). Αντίστοιχα, αναλόγως με τους κανόνες και τα όρια που έχουν τεθεί από τον Εκδότη, το chip θα απαντήσει με μία από τις εξής εντολές ARQC: go online, AAC: offline decline, TC: offline approval. Στην περίπτωση που ζητηθεί από το chip να γίνει online η επεξεργασία της συναλλαγής, τότε το τερματικό EFT/POS στέλνει online αίτημα στον Εκδότη ώστε να γίνει η αυθεντικοποίηση της κάρτας. Εάν η απάντηση περιλαμβάνει προαιρετική αυθεντικοποίηση από τον Εκδότη (ARPC), τότε το τερματικό EFT/POS θα στείλει τα δεδομένα στο chip για επιβεβαίωση. Σε αυτό το στάδιο, η συναλλαγή ολοκληρώνεται. Σε περίπτωση που επιλέχθηκε η online επεξεργασία της συναλλαγής, το chip θα πρέπει να επιβεβαιώσει με απάντηση TC είτε AAC και να εφαρμόσει τις αντίστοιχες εντολές όπως έχουν οριστεί από τον Εκδότη.

5.2 ΕΠΙΚΟΙΝΩΝΙΑ

Η βασικότερη διαφορά μεταξύ μίας ανέπαφης συναλλαγής με chip και μίας συναλλαγής με επαφή, είναι ότι η μετάδοση των πληροφοριών που πραγματοποιείται μεταξύ chip και τερματικού EFT/POS είναι ταχύτερη για την ανέπαφη και ορισμένα βήματα εκτελούνται αφού πλέον το chip (επομένως η κάρτα) έχει απομακρυνθεί από την εμβέλεια του αναγνώστη. Ένα παράδειγμα τέτοιου βήματος αποτελεί το online authorization.

Συγκεκριμένα, η επικοινωνία μεταξύ της κάρτας και του τερματικού EFT/POS πραγματοποιείται με τη μέθοδο half duplex: Μόνο το ένα μέρος μπορεί να μεταδίδει σε μία δεδομένη στιγμή, ενώ το άλλο πρέπει να περιμένει να τερματίσει μια μετάδοση, προτού να μπορέσει να απαντήσει πίσω. Το τερματικό EFT/POS είναι υπεύθυνο για να ξεκινήσει την επικοινωνία με την κάρτα και να ζητήσει πληροφορίες. Για να γίνει αυτό, υλοποιεί εντολές. Χρησιμοποιείται το πρωτόκολλο επικοινωνίας APDU (Application Protocol Data Unit). Το πρωτόκολλο APDU είναι ένα σύνολο εντολών που το τερματικό EFT/POS και η κάρτα εφαρμόζουν για αλληλεπίδραση μεταξύ τους.

5.3 ΑΣΦΑΛΕΙΑ - ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΚΑΡΤΑΣ

Όπως γίνεται κατανοητό από τη διαδικασία της συναλλαγής όπως αυτή περιγράφεται στα παραπάνω κεφάλαια, έχουν οριστεί διάφορες λειτουργίες μέσω των οποίων προστατεύονται οι κάτοχοι των καρτών, οι έμποροι αλλά και οι εκδότες (Τράπεζες, κ.λπ.). Σκοπό όλων αυτών των ελέγχων αποτελεί ο περιορισμός της απάτης με χρήση πλαστών ή κλεμμένων καρτών. Παρακάτω θα αναλυθούν λειτουργίες όπως το Κρυπτογράφημα εφαρμογής (Application Cryptogram), η διαχείριση ρίσκου και οι έλεγχοι εξουσιοδότησης, η επιβεβαίωση του κατόχου της κάρτας (Cardholder Verification Processing) αλλά και η διαδικασία του Offline Data Authentication.

5.3.1 APPLICATION CRYPTOGRAMS

Το κρυπτογράφημα εφαρμογής παράγεται με τη χρήση διπλού κλειδιού triple DES. Η συγκεκριμένη υπογραφή παράγεται από σημαντικά δεδομένα που περιέχονται είτε στο αίτημα για online authorization προς τον Εκδότη της κάρτας, είτε στην τελική χρηματική συναλλαγή (Clearing and Settlement: ανανέωση του κάθε τραπεζικού λογαριασμού ώστε να φαίνεται η νέα συναλλαγή και ύστερα το πραγματικό χρηματικό ποσό μεταφέρεται από τον έναν τραπεζικό λογαριασμό στον άλλον). Το κρυπτογράφημα που παράγεται για το αίτημα του online authorization είναι γνωστό ως Authorization Request Cryptogram (ARQC) ενώ το κρυπτογράφημα που παράγεται όταν το chip αποδέχεται την τελική χρηματική συναλλαγή,

ονομάζεται Transaction Certificate (TC). Σε περίπτωση απόρριψης της συναλλαγής, το chip θα παράγει ένα κρυπτογράφημα γνωστό ως Application Authentication Cryptogram (AAC).

Σκοπός αυτών των κρυπτογραφημάτων αποτελεί η online αυθεντικοποίηση κάρτας και εκδότη αλλά και η υπογραφή των στοιχείων της συναλλαγής με σκοπό την αυθεντικοποίηση και την εξασφάλιση της ακεραιότητάς της.

5.3.1.1 ONLINE CARD AND ISSUER AUTHENTICATION

Το chip παράγει ένα ARQC το οποίο στέλνεται στο αίτημα εξουσιοδότησης όταν η συναλλαγή συνεχίζει online στον εκδότη. Η επαλήθευση του ARQC πραγματοποιείται από τον εκδότη και με αυτόν τον τρόπο επιβεβαιώνεται πως το chip δεν είναι πλαστό. Ο εκδότης, μπορεί να παράγει ένα κρυπτογράφημα γνωστό ως Authorization Response Cryptogram (ARPC) το οποίο στέλνεται πίσω στο chip στο authorization response. Η αποστολή του ARPC επιτρέπει στο chip να επιβεβαιώσει πως η αποδοχή στάλθηκε από τον πραγματικό εκδότη.

5.3.1.1 ΥΠΟΓΡΑΦΗ ΤΩΝ ΣΤΟΙΧΕΙΩΝ - ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ

Η διαδικασία της αυθεντικοποίησης της κάρτας πραγματοποιείται σε ένα τερματικό EFT/POS και έχει ως στόχο να αποδείξει στον εκδότη ότι η κάρτα περιέχει ένα έγκυρο, γνήσιο και μοναδικό κλειδί. Τα κρυπτογραφήματα ARQC, ARPC, TC και AAC όπως έχει αναφερθεί και παραπάνω, παράγονται από την υπογραφή των σημαντικών στοιχείων στα εκάστοτε μηνύματα συναλλαγών. Η επαλήθευση των κρυπτογραφημάτων από τον παραλήπτη συμβάλλει στο να επιβεβαιωθεί πως δεν έχουν αλλαχθεί τα δεδομένα.

Η όλη διαδικασία απαιτεί από το τερματικό EFT/POS να ζητά από την κάρτα ένα κρυπτογράφημα (AC). Μία μορφή κρυπτογραφήματος εφαρμογής μπορεί να είναι το κρυπτογράφημα Authorisation Request Cryptogram (ARQC). Μαζί με το αίτημα, το τερματικό EFT/POS στέλνει επίσης ένα ‘challenge’ στην κάρτα. Αν η κάρτα αποφασίσει να προχωρήσει on-line, χρησιμοποιεί το συμμετρικό κλειδί που μοιράζεται με τον εκδότη και προσθέτει ένα Message Authentication Code (MAC) για να συνοδεύσει τον αριθμό των μηνυμάτων (Σχήμα 5.1). Το μήνυμα ARQC προωθείται στο τερματικό EFT/POS, και το τελευταίο με τη σειρά του το προωθεί στον εκδότη.

Value	Source
Amount, Authorised (Numeric)	Terminal
Amount Other (Numeric)	Terminal
Terminal Country Code	Terminal
Terminal Verification Results	Terminal
Transaction Currency Code	Terminal
Transaction Date	Terminal
Transaction Type	Terminal
Unpredictable Number	Terminal
Application Interchange Profile	smart card
Application Transaction Counter (ATC)	smart card

Σχήμα 5.1: Μηνύματα που υποστηρίζονται από την ARQC

Ο εκδότης χρησιμοποιεί το κοινό κλειδί, προκειμένου να επαληθεύσει το κρυπτογράφημα ARQC. Στη συνέχεια, ενημερώνει το τερματικό EFT/POS εάν η συναλλαγή είναι εγκεκριμένη ή όχι. Η πραγματοποίηση ή μη της συναλλαγής εξαρτάται από την επιτυχή επαλήθευση του κρυπτογραφήματος ARQC, από το χρηματικό ποσό που διαθέτει ο λογαριασμός της κάρτας αλλά και άλλους τυπικούς ελέγχους (π.χ. ότι η κάρτα δεν έχει δηλωθεί ως κλεμμένη). Συμπεριλαμβανομένων, των δεδομένων που παρουσιάζονται στον παραπάνω πίνακα (Σχήμα 5.3), ο εκδότης μπορεί να επιβεβαιώσει ότι τα δεδομένα δεν έχουν αλλάξει κατά τη διαδικασία και κυρίως ότι η συναλλαγή επιτρέπεται ταυτόχρονα με την επικύρωση/αυθεντικοποίηση της κάρτας.

Ο μετρητής των συναλλαγών Application Transaction Counter (ATC) βρίσκεται στην κάρτα και αυξάνεται κάθε φορά που πραγματοποιείται μια συναλλαγή. Δεδομένου ότι ο μετρητής ATC είναι διαφορετικός για κάθε συναλλαγή, το κρυπτογράφημα που προκύπτει θα είναι επίσης διαφορετικό. Ο κύριος στόχος του μετρητή ATC είναι η αποφυγή των επιθέσεων τύπου reply.

Το κρυπτογράφημα ARPC μπορεί να σταλεί στην απάντηση εξουσιοδότησης από τον εκδότη στην κάρτα μέσω του τερματικού EFT/POS. Όταν η κάρτα παραλαμβάνει το κρυπτογράφημα ARPC, είναι σε θέση να επιβεβαιώσει ότι πρόκειται για απάντηση στο μήνυμά της και ότι προέρχεται από τον εκδότη καθώς για το συγκεκριμένο κρυπτογράφημα χρησιμοποιείται triple DES MAC αλγόριθμος. Το κρυπτογράφημα ARPC συνδέεται με το κρυπτογράφημα ARQC (και τον μετρητή ATC), επομένως, τυχόν απόπειρες χειρισμού της κάρτας με επανάληψη των ήδη εκδοθεισών εντολών ARPC, θα αποτύχουν.

5.3.2 ΔΙΑΧΕΙΡΙΣΗ ΡΙΣΚΟΥ ΚΑΙ ΕΛΕΓΧΟΙ ΕΞΟΥΣΙΟΔΟΤΗΣΗΣ

Οι Τράπεζες που εκδίδουν τις κάρτες, θέτουν όρια στο chip περιορίζοντας με αυτόν τον τρόπο τον αριθμό των διαδοχικών offline συναλλαγών που μπορούν πραγματοποιηθούν. Επιπροσθέτως, μέσω κάποιων εντολών που μπορούν να σταλούν στην κάρτα κατά τη διάρκεια μίας απάντησης online authorization, ο εκδότης μπορεί να αλλάξει τα όρια της κάρτας, ακόμα

και να τα μηδενίσει ανάλογα με την εκτίμηση ρίσκου. Υπάρχει και η δυνατότητα διακοπής λειτουργίας ή και απενεργοποίησης μίας χαμένης ή κλεμμένης κάρτας. Επίσης, η επιλογή των συναλλαγών που θα μεταφερθούν online για έγκριση μπορεί να βασιστεί όχι μόνο στο floor limit αλλά και σε άλλα κριτήρια (ανάλογα με τη χώρα στην οποία πραγματοποιείται η συναλλαγή ή ανά το εκάστοτε κατάστημα/επιχείρηση). Τέλος, ορισμένες συναλλαγές, ακόμα και μικρότερου ποσού από το floor limit μπορεί να επιλεχθούν τυχαία και να αποσταλούν online στα πλαίσια ελέγχου.

5.3.3 ΕΞΑΚΡΙΒΩΣΗ ΤΟΥ ΚΑΤΟΧΟΥ ΤΗΣ ΚΑΡΤΑΣ

Σε αυτό το υποκεφάλαιο, θα αναφερθούν δύο λειτουργίες οι οποίες βοηθούν στην μείωση της απάτης από χαμένες είτε κλεμμένες κάρτες. Η πρώτη λειτουργία είναι η Cardholder Verification Method (CVM) λίστα. Μέσω αυτής, ο εκδότης μπορεί να προσδιορίσει σε σειρά ποιες μέθοδοι επιβεβαίωσης του κατόχου της κάρτας θα εφαρμοστούν. Ανάλογα με το ποια CVM μέθοδος υποστηρίζεται από το τερματικό EFT/POS, επιλέγεται και ποια θα εφαρμοστεί αντίστοιχα. Για παράδειγμα, σε περίπτωση που δεν υποστηρίζεται η χρήση κωδικού PIN σε κάποιο τερματικό EFT/POS, τότε πρέπει να υπάρχει εναλλακτική για τον κάτοχο της κάρτας, όπως η δυνατότητα υπογραφής. Η δεύτερη CVM λειτουργία αφορά το offline PIN. Μέσω του chip της κάρτας μπορεί να επαληθευθεί το PIN που έχει εισαχθεί στο τερματικό EFT/POS είτε πρόκειται για offline είτε για online συναλλαγή. Υπάρχουν δύο βασικές παραλλαγές του ελέγχου PIN εκτός σύνδεσης (off-line PIN). Την πρώτη αποτελεί η μετάδοση του PIN (με την εντολή VERIFY) χωρίς χρήση κρυπτογράφησης από το τερματικό EFT/POS στις έξυπνες κάρτες, για έλεγχο. Υπάρχει επίσης η δυνατότητα κρυπτογράφησης, χρησιμοποιώντας το δημόσιο κλειδί κάρτας, τον κωδικό PIN και, στη συνέχεια, την αποστολή στην κάρτα μέσω της εντολής VERIFY. Η κάρτα θα χρησιμοποιήσει τότε το ιδιωτικό κλειδί της, για να αποκρυπτογραφήσει το μήνυμα και να επαληθεύσει το PIN.

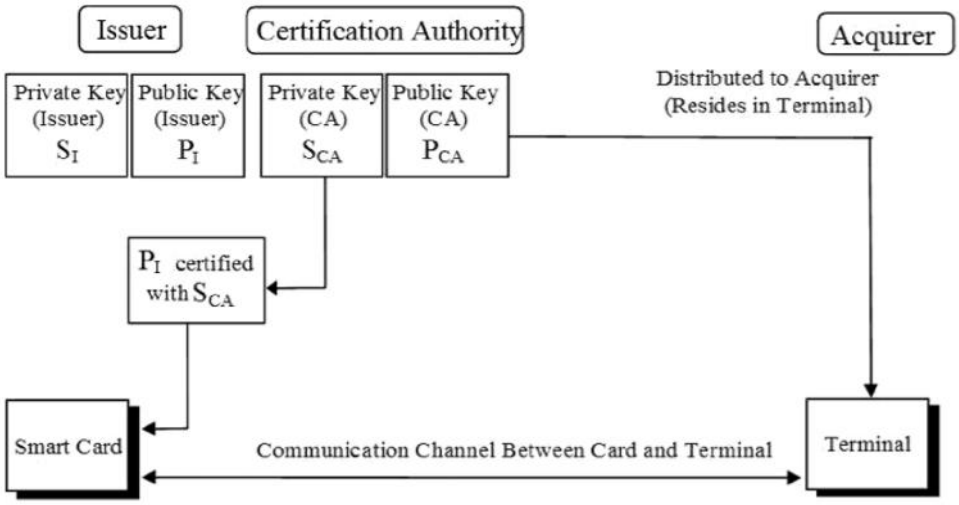
5.3.4 OFFLINE DATA AUTHENTICATION

Για την αυθεντικοποίηση της κάρτας, το τερματικό EFT/POS εκτελεί ορισμένους ελέγχους για να εξακριβώσει αν η κάρτα έχει υποστεί κάποια αλλαγή με μη εξουσιοδοτημένο τρόπο από την αρχή της έκδοσης της. Αυτοί οι έλεγχοι δύναται να πραγματοποιηθούν χωρίς να χρειαστεί να πραγματοποιηθεί online έλεγχος από τον εκδότη. Όταν η έξυπνη κάρτα εισάγεται στο τερματικό EFT/POS, οι δύο οντότητες ξεκινούν ένα διάλογο. Όπως αναφέρθηκε και παραπάνω, η απόφαση για τη διεξαγωγή ή μη της συναλλαγής, βασίζεται σε ορισμένες παραμέτρους όπως η αξίας της συναλλαγής, ο αριθμός των off-line συναλλαγών κλπ. Οι EMV προδιαγραφές καθορίζουν τρεις διαφορετικές μεθόδους αυθεντικοποίησης οι οποίες είναι οι Static Data

Authentication (SDA), Dynamic Data Authentication (DDA) και Combined Data Authentication (CDA). Η τελευταία αποτελεί μία παραλλαγή της Dynamic Data Authentication μεθόδου.

5.3.4.1 STATIC DATA AUTHENTICATION (SDA)

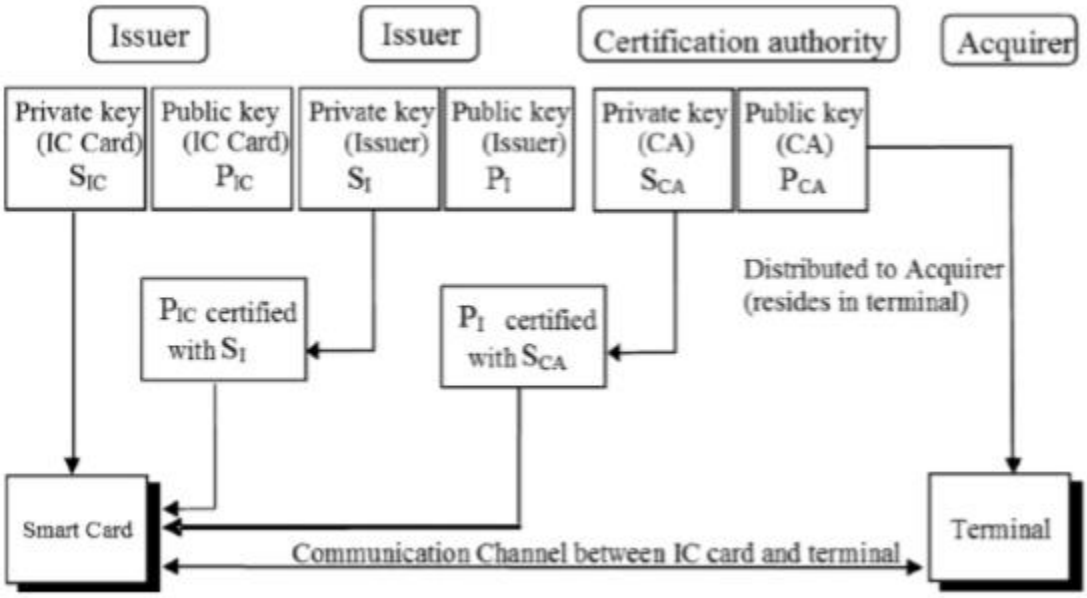
Η όλη διαδικασία του SDA βασίζεται στην ύπαρξη μιας αρχής πιστοποίησης (π.χ. Visa, MasterCard, κλπ. (EMV) – γνωστές και ως scheme operator). Ο εκδότης δημιουργεί ένα ζεύγος δημόσιου και ιδιωτικού κλειδιού. Η αρχή πιστοποίησης (EMV) δημιουργεί το δικό της ζεύγος ιδιωτικού και δημόσιου κλειδιού και χρησιμοποιώντας το ιδιωτικό κλειδί του συστήματος, πιστοποιεί το δημόσιο κλειδί του εκδότη που βρίσκεται τοποθετημένο στην κάρτα EMV. Το δημόσιο κλειδί της αρχής πιστοποίησης τοποθετείται σε κάθε συμμετέχον τερματικό EFT/POS. Στη συνέχεια, ο εκδότης υπογράφει ορισμένα στατικά δεδομένα της κάρτας χρησιμοποιώντας το ιδιωτικό του κλειδί και τοποθετεί την υπογραφή που προκύπτει στην κάρτα (κατά τη διάρκεια της φάσης εξατομίκευσης). Κατά τη διάρκεια μίας συναλλαγής με κάρτα EMV η οποία υποστηρίζει SDA αυθεντικοποίηση, το τερματικό EFT/POS ανακτά το δημόσιο κλειδί του συστήματος για να επαληθεύσει το δημόσιο κλειδί του εκδότη. Στη συνέχεια, χρησιμοποιεί το δημόσιο κλειδί του εκδότη, προκειμένου να επαληθεύσει την υπογραφή του εκδότη στα δεδομένα της κάρτας. Αν η διαδικασία ολοκληρωθεί χωρίς προβλήματα, το τερματικό EFT/POS λαμβάνει την επιβεβαίωση ότι τα δεδομένα της κάρτας δεν έχουν τροποποιηθεί κατά τη διάρκεια που η κάρτα είναι σε λειτουργία.



Σχήμα 5.2 Συναλλαγή με αυθεντικοποίηση τύπου Static Data (SDA)

5.3.4.2 DYNAMIC DATA AUTHENTICATION (DDA)

Κατά τη διάρκεια μιας συναλλαγής DDA, η κάρτα παράγει μία ψηφιακή υπογραφή (με λεπτομέρειες της συναλλαγής και συγκεκριμένα στοιχεία της κάρτας) χρησιμοποιώντας ένα μυστικό κλειδί (το οποίο έχει δημιουργήσει ο εκδότης). Κάθε κάρτα διαθέτει επίσης πιστοποιητικό (που παράγεται από τον εκδότη) το οποίο περιέχει το αντίστοιχο δημόσιο κλειδί της κάρτας. Αυτό το πιστοποιητικό δημιουργείται χρησιμοποιώντας το ιδιωτικό κλειδί του εκδότη. Το αντίστοιχο δημόσιο κλειδί του εκδότη πιστοποιείται από το ιδιωτικό κλειδί της αρχής πιστοποίησης. Το δημόσιο κλειδί της αρχής πιστοποίησης βρίσκεται σε όλα τα συμμετέχοντα τερματικά EFT/POS. Επομένως, εάν μία κάρτα που υποστηρίζει DDA ζητά να «συμμετάσχει» σε μια συναλλαγή, θα της ζητηθεί να υπογράψει συγκεκριμένες λεπτομέρειες. Το τερματικό EFT/POS, έχοντας πρόσβαση στο δημόσιο κλειδί της αρχής πιστοποίησης θα μπορέσει να επαληθεύσει το δημόσιο κλειδί του εκδότη και κατ' επέκταση το δημόσιο κλειδί της κάρτας. Το δημόσιο κλειδί της κάρτας θα χρησιμοποιηθεί ώστε να επαληθεύσει τις υπογραφές της κάρτας με σκοπό τελικά να ελέγξει ότι τα υπογεγραμμένα δεδομένα προέρχονται από μια νόμιμη κάρτα.



Σχήμα 5.3 Συναλλαγή με αυθεντικοποίηση τύπου Dynamic Data (DDA)

5.3.4.3 COMBINED DATA AUTHENTICATION (CDA)

Μια περαιτέρω βελτίωση στην αυθεντικοποίηση των δεδομένων αποτελεί η μεθόδους του Combined Data Authentication (CDA). Το CDA συνδυάζει μια δυναμική υπογραφή και ένα κρυπτογράφημα εφαρμογής. Η κύρια διαφορά μεταξύ του CDA και του DDA είναι ότι μέρος των δεδομένων που θα υπογραφεί από την έξυπνη κάρτα, περιλαμβάνει επίσης ένα κρυπτογράφημα (Application Request Cryptogram - ARQC) και τον τυχαίο αριθμό που παρέχεται από το τερματικό EFT/POS. Έχει σχεδιαστεί με σκοπό την αντιμετώπιση μίας μεθόδου επίθεσης στα τερματικά EFT/POS κατά την οποία ο επιτιθέμενος προσπαθεί να χρησιμοποιήσει μία έγκυρη chip κάρτα ώστε να ξεπεράσει το σημείο που πραγματοποιείται το offline data authentication και από εκεί να προσομοιώσει ενέργειες που πραγματοποιεί μία κάρτα με σκοπό να αποκτήσει εξουσιοδότηση.

Η βασική διαφορά μεταξύ SDA και DDA είναι πως η πρώτη εξασφαλίζει μεν ότι τα δεδομένα του chip δεν έχουν υποστεί κάποια αλλαγή από την έκδοση της εκάστοτε κάρτας, αλλά δεν εξασφαλίζει απαραίτητα και τη γνησιότητα της κάρτας. Η αντιγραφή των δεδομένων του chip μαζί με το SDA κρυπτογράφημα είναι πιθανή και αποσκοπεί στη δημιουργία ενός άλλου chip το οποίο θα μπορούσε να περάσει επιτυχώς το offline SDA (δεδομένου ότι πλαστές κάρτες ανιχνεύονται σε περίπτωση online επεξεργασίας). Καταληκτικά, η DDA μέθοδος αποτελεί ισχυρότερη μέθοδο offline αυθεντικοποίησης αφού κατά τον έλεγχο χρησιμοποιεί μοναδικά δεδομένα της κάθε συναλλαγής.

5.3.4.4 TRANSACTION CERTIFICATE

Το Πιστοποιητικό Συναλλαγών (Transaction Certificate - TC) πρόκειται για ένα κρυπτογράφημα το οποίο δείχνει εάν μια συναλλαγή εγκρίθηκε ή όχι. Το TC παρέχει επίσης πρόσθετες πληροφορίες σχετικά με τη διαβίβαση καθ’ όλη τη διάρκεια της συναλλαγής. Όλες αυτές οι πληροφορίες είναι ιδιαίτερα χρήσιμες σε περίπτωση διαφωνίας αφού ο έμπορος μπορεί να τις χρησιμοποιήσει ως απόδειξη του ότι η κάρτα έχει δεχθεί μία συναλλαγή. Ολόκληρη η διαδικασία επιτυγχάνεται ζητώντας από την κάρτα να παράγει ένα κρυπτογράφημα DES σε συγκεκριμένα δεδομένα συναλλαγής (π.χ. εάν το τερματικό EFT/POS χρησιμοποιεί αυθεντικοποίηση SDA ή DDA, κρυπτογράφημα ARQC, αν η εξουσιοδότηση ήταν on-line, κ.λπ.). Αυτές οι πληροφορίες παρέχονται από την κάρτα στον εκδότη μέσω του τερματικού EFT/POS. [9], [14]

5.4 ΠΡΩΤΟΚΟΛΛΟ ΕΠΙΚΟΙΝΩΝΙΑΣ

Η επικοινωνία μεταξύ αναγνώστη και κάρτας, επιτυγχάνεται μέσω των APDU (Application Protocol Data Unit) εντολών. Η δομή του έχει οριστεί μέσω του προτύπου ISO 7816. Υπάρχουν δύο κατηγορίες APDUs, οι εντολές APDUs και οι απαντήσεις APDUs. Η πρώτη κατηγορία αφορά την επικοινωνία που στέλνεται από τον αναγνώστη στην κάρτα. Περιλαμβάνει υποχρεωτικά έναν 4-byte header (CLA, INS, P1, P2) και από 0 – 255 bytes δεδομένων. Η δεύτερη κατηγορία αφορά την επικοινωνία από την κάρτα στον αναγνώστη και πρέπει να περιλαμβάνει μία λέξη των 2 byte (SW1, SW2) και 0 – 255 bytes δεδομένων.

5.5 EMV ΣΤΗΝ ΠΡΑΞΗ

Οι διαχειριστές των συστημάτων είναι υπεύθυνοι για την ενημέρωση των τραπεζών-μελών τους σχετικά με τις απαραίτητες οδηγίες για την ορθή εφαρμογή του EMV. Η αφύπνιση των

χρηματοπιστωτικών οργανισμών ώστε να είναι σε θέση να κατανοήσουν τα οικονομικά οφέλη από τον περιορισμό της απάτης είναι ιδιαίτερα σημαντική. Σε ορισμένες περιοχές, οι φορείς εκμετάλλευσης των συστημάτων παρείχαν επίσης προγράμματα παροχής κινήτρων για τη χρήση καρτών με τσιπ. Για παράδειγμα, προσφορά για την κάλυψη μέρους του κόστους κάθε κάρτας με ενσωματωμένο επεξεργαστή (chip) που θα αντικαταστήσει μια κάρτα μαγνητικής λωρίδας.

Πρέπει να αναφερθεί ότι μέχρι το 2001 η πλειοψηφία των εκδοθέντων καρτών EMV υποστήριζε την μέθοδο αυθεντικοποίησης SDA. Το DDA ήταν διαθέσιμο, αλλά το κόστος της κάρτας ήταν σχετικά απαγορευτικό. Οι εκδότες έπρεπε επίσης να λάβουν υπόψη το συνολικό κόστος των απαιτούμενων αλλαγών στα τερματικά EFT/POS, κυρίως όσον αφορά τις νέες εφαρμογές και τη σύνδεση επικοινωνίας με τον λήπτη. Ως εκ τούτου, αποφασίστηκε ότι το SDA θα χρησιμοποιηθεί για αρχή. Αφού αποκτήθηκε η απαιτούμενη εμπειρία και μειώθηκαν οι δαπάνες όσον αφορά τις τηλεπικοινωνίες και την κάρτα (υποστηρίζοντας την κρυπτογραφία δημόσιου κλειδιού), μπόρεσαν να υιοθετηθούν εναλλακτικές λύσεις. [14]

ΚΕΦΑΛΑΙΟ 6^{ο} - ΠΕΙΡΑΜΑΤΑ

6.1 EAVESDROPPING ΜΕ ΤΗ ΧΡΗΣΗ ΑΥΤΟΣΧΕΔΙΑΣ ΚΕΡΑΙΑΣ

Ο σκοπός του πειράματος ήταν να αποδειχθεί ότι είναι δυνατή η ανάκτηση πληροφοριών που αποστέλλονται μεταξύ συσκευών NFC με τη χρήση απλού εξοπλισμού. Η συγκεκριμένη κακόβουλη ενέργεια μάλιστα, είναι ανεξάρτητη της μικρής εμβέλειας στην οποία μπορεί να επικοινωνήσει ο αναγνώστης με την κάρτα για την πραγματοποίηση της συναλλαγής.

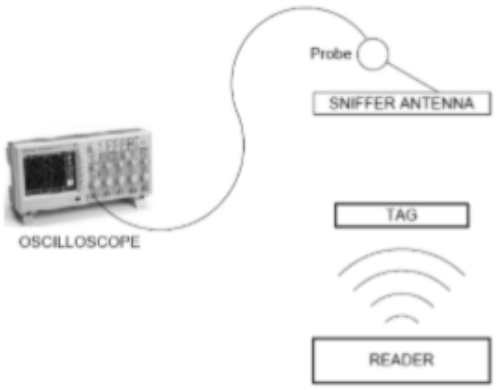
Αυτό συμβαίνει καθώς η απόσταση στην οποία μπορεί μια κεραία να λάβει το σήμα επικοινωνίας μεταξύ του αναγνώστη και της κάρτας είναι αρκετά μεγαλύτερη από την απόσταση ώστε να είναι εφικτή η τροφοδοσία και άρα η λειτουργία της κάρτας. Με λίγα λόγια από τη στιγμή που η κάρτα τροφοδοτείται από τον αναγνώστη είναι δυνατόν να «ακούσουμε» την μεταξύ τους επικοινωνία από πολύ μεγαλύτερη απόσταση.

Με αυτόν τον τρόπο, αποδεικνύεται ότι η εγγύτητα της NFC τεχνολογίας η οποία πολλές φορές αναφέρεται και ως μέτρο ασφάλειας σε ορισμένα σενάρια δεν αρκεί για να διασφαλίσει από μόνη της την ασφάλεια της επικοινωνίας ανάμεσα σε κάρτες και αναγνώστη.

6.1.1 ΜΕΘΟΔΟΣ ΠΕΙΡΑΜΑΤΟΣ

Αρχικά, επιχειρήθηκε η παρατήρηση του σχήματος διαμόρφωσης και κωδικοποίησης τόσο του downlink όσο και του uplink καναλιού ώστε να δούμε πως εφαρμόζεται στην πράξη το πρότυπο ISO14443-2. Στη συνέχεια, εντοπίζονται ο τρόπος με τον οποίο αναπαρίστανται τα λογικά «0» και «1». Το επόμενο βήμα ήταν να αναγνωρίσουμε πλήρεις εντολές από τις ακολουθίες των ψηφίων και να ελέγξουμε αν συμφωνούν με τις ακολουθίες επικοινωνίας όπως αυτές περιγράφονται στα πρότυπα. Τέλος, έγινε προσπάθεια καθορισμού της μέγιστης απόστασης από την οποία ήταν δυνατή η υποκλοπή σήματος με τον εξοπλισμό που είχαμε στη διάθεσή μας και να το συγκρίνουμε με την απόσταση λειτουργίας.

Στο Σχήμα 6.1 απεικονίζεται η πειραματική ρύθμιση για την υποκλοπή μετάδοσης δεδομένων μεταξύ ενός αναγνώστη NFC και μιας ετικέτας NFC χρησιμοποιώντας ένα παλμογράφο και μια αυτοσχέδια κεραία.

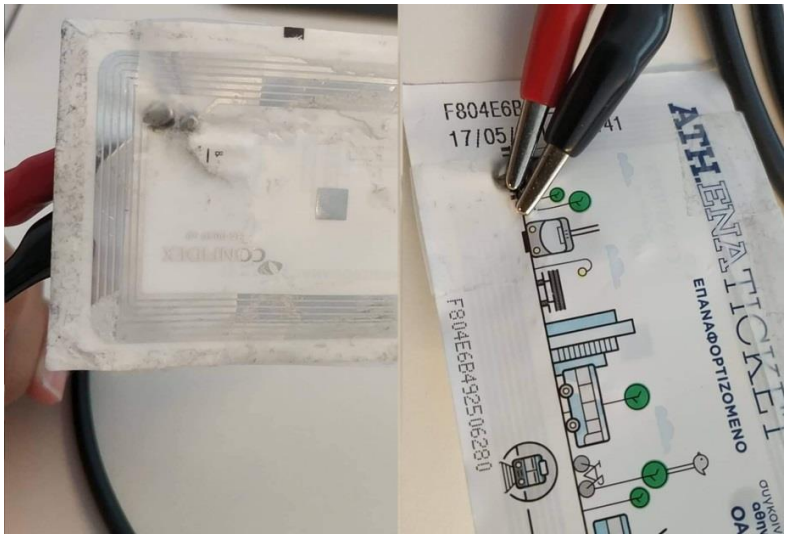


Σχήμα 6.1: Σχηματικό της διάταξης

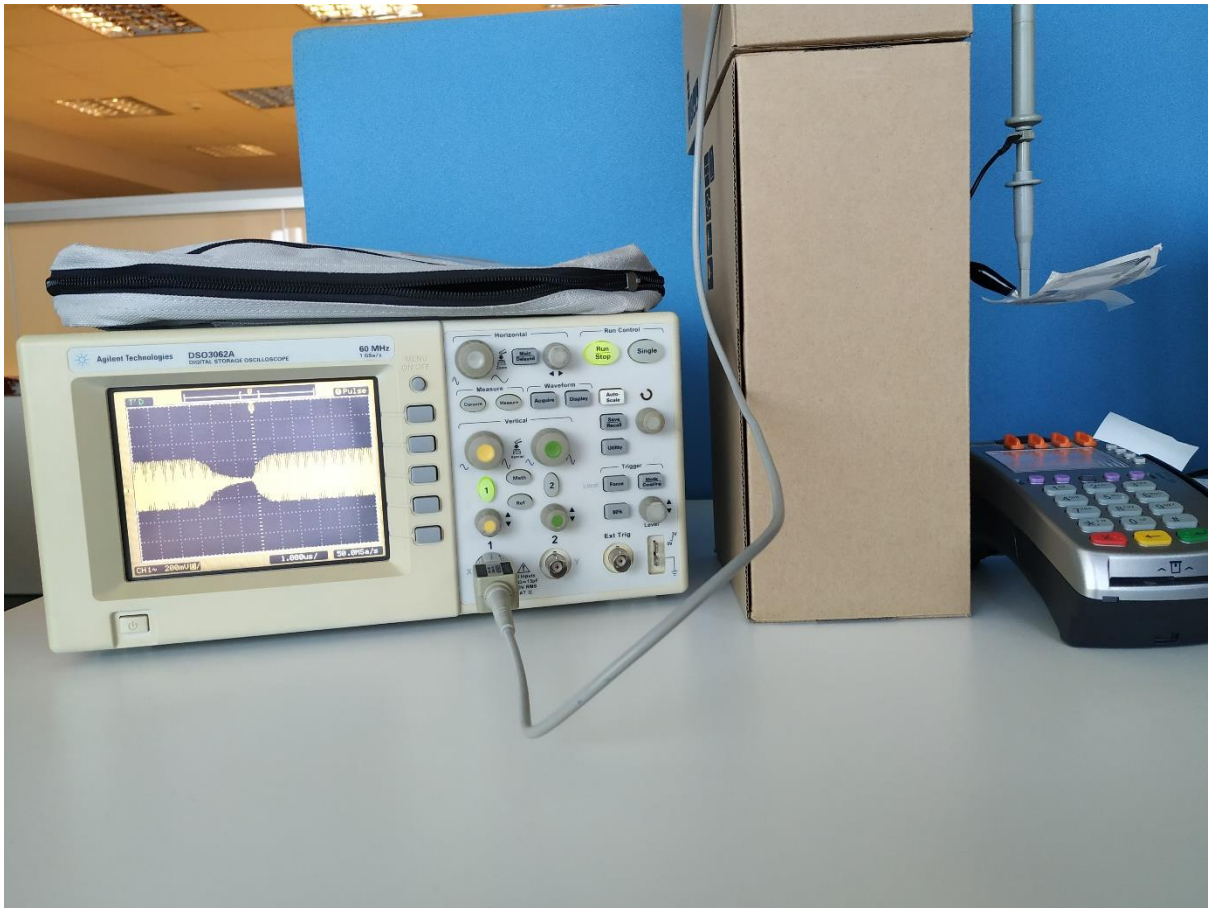
6.1.2 ΠΕΙΡΑΜΑΤΙΚΟΣ ΕΞΟΠΛΙΣΜΟΣ

Τα πειράματα πραγματοποιήθηκαν με τη χρήση ενός αναγνώστη, μιας ετικέτας και μια παθητική κεραία συνδεδεμένη σε έναν παλμογράφο. Ο αναγνώστης NFC που χρησιμοποιήθηκε σε αυτό το πείραμα ήταν ένα test EFT/POS. Επίσης χρησιμοποιήθηκε μία test πιστωτική/χρεωστική κάρτα τύπου Α η οποία αποτέλεσε το στόχο της επίθεσης.

Η αυτοσχέδια κεραία είναι μία ετικέτα MIFARE και είχε το ρόλο του κακόβουλου ωτακουστή. Στην πράξη, πρόκειται για ένα τροποποιημένο εισιτήριο ΟΑΣΑ, RFID τεχνολογίας, η οποία είναι συμβατή με την NFC τεχνολογία. Το γεγονός αυτό διασφαλίζει πως ο σχεδιασμός της κεραίας είναι κατάλληλος για τη δική μας εφαρμογή. Για τη χρήση της αυτοσχέδιας κεραίας, χρειάστηκε να αφαιρέσουμε τη χάρτινη και πλαστική επίστρωση αλλά και το ολοκληρωμένο chip που βρισκόταν συνδεδεμένο στα άκρα της. Για την ανάλυση των σημάτων RF, χρησιμοποιήθηκε ένας ψηφιακός παλμογράφος Agilent Technologies DSO3062A (60MHz) στου οποίου τα άκρα συνδέσαμε την αυτοσχέδια κεραία.



Σχήμα 6.2: Αυτοσχέδια Κεραία



Σχήμα 6.3: Διάταξη για την πραγματοποίηση του Πειράματος

6.1.3 ΡΥΘΜΙΣΕΙΣ ΠΑΛΜΟΓΡΑΦΟΥ

Για τη λειτουργία του παλμογράφου, την εύρεση και καταγραφή των επιθυμητών αποτελεσμάτων, ρυθμίστηκαν τα εξής:

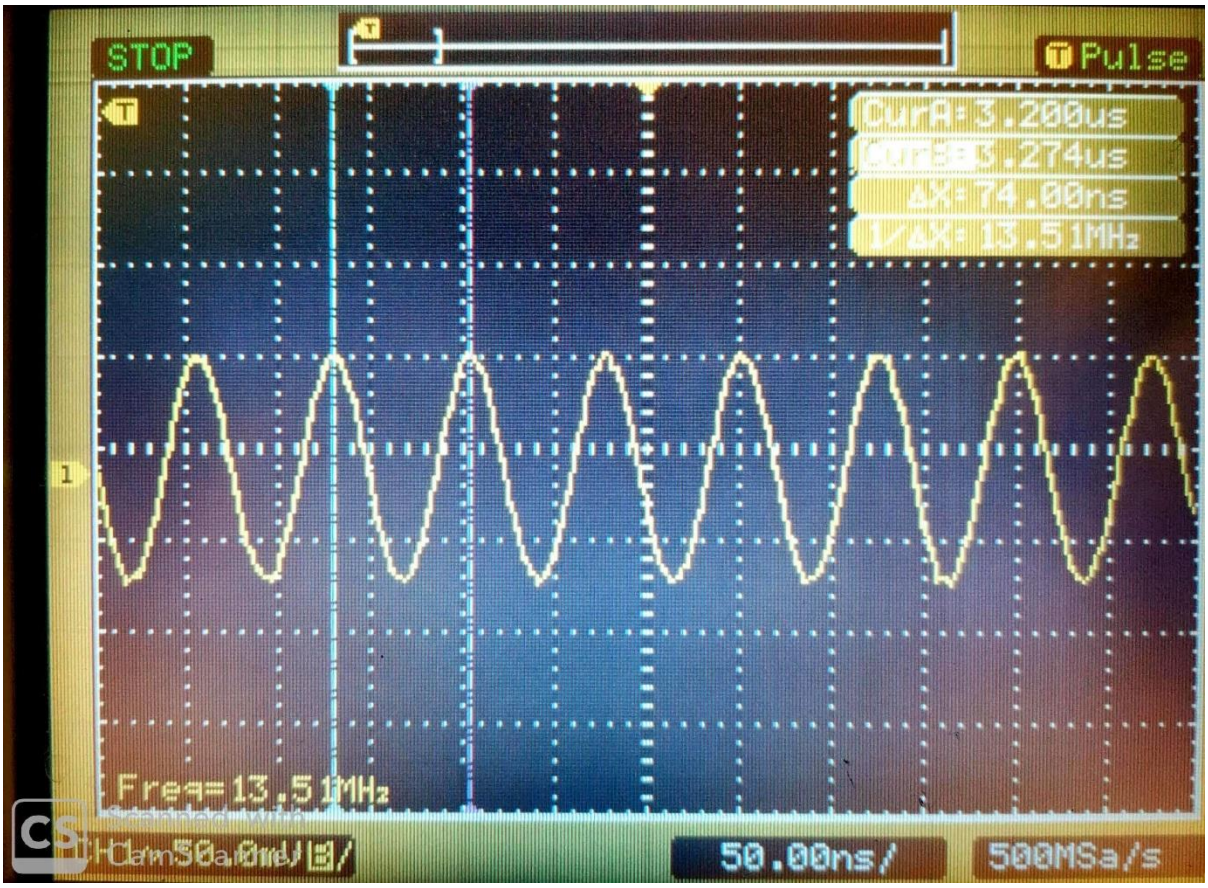
- Trigger → Mode/Coupling (ρύθμιση η οποία αφορά βάσει ποιου τρόπου θα ξεκινήσουν οι μετρήσεις)
- Mode → Pulse
- Source → CH1
- Trigger Level → 0
  Το συμβάν το οποίο ανιχνεύει ο παλμογράφος, είναι ένας παλμός διάρκειας μεγαλύτερης (>) των 2 μs.
  Η συγκεκριμένη συνθήκη βρέθηκε πως ικανοποιείται μόνο στην αρχή της REQA εντολής. Επομένως, με τις συγκεκριμένες ρυθμίσεις, βλέπουμε την αρχή της.
- Ενεργοποίηση του bandwidth Limit. Με αυτόν τον τρόπο εφαρμόζεται ένα φίλτρο, το οποίο αποτρέπει το θόρυβο.

Οι παραπάνω ρυθμίσεις ενεργοποιούνται πάντα κατά τον πρώτο παλμό ASK.

6.1.4 ΠΕΙΡΑΜΑΤΙΚΗ ΔΙΑΔΙΚΑΣΙΑ

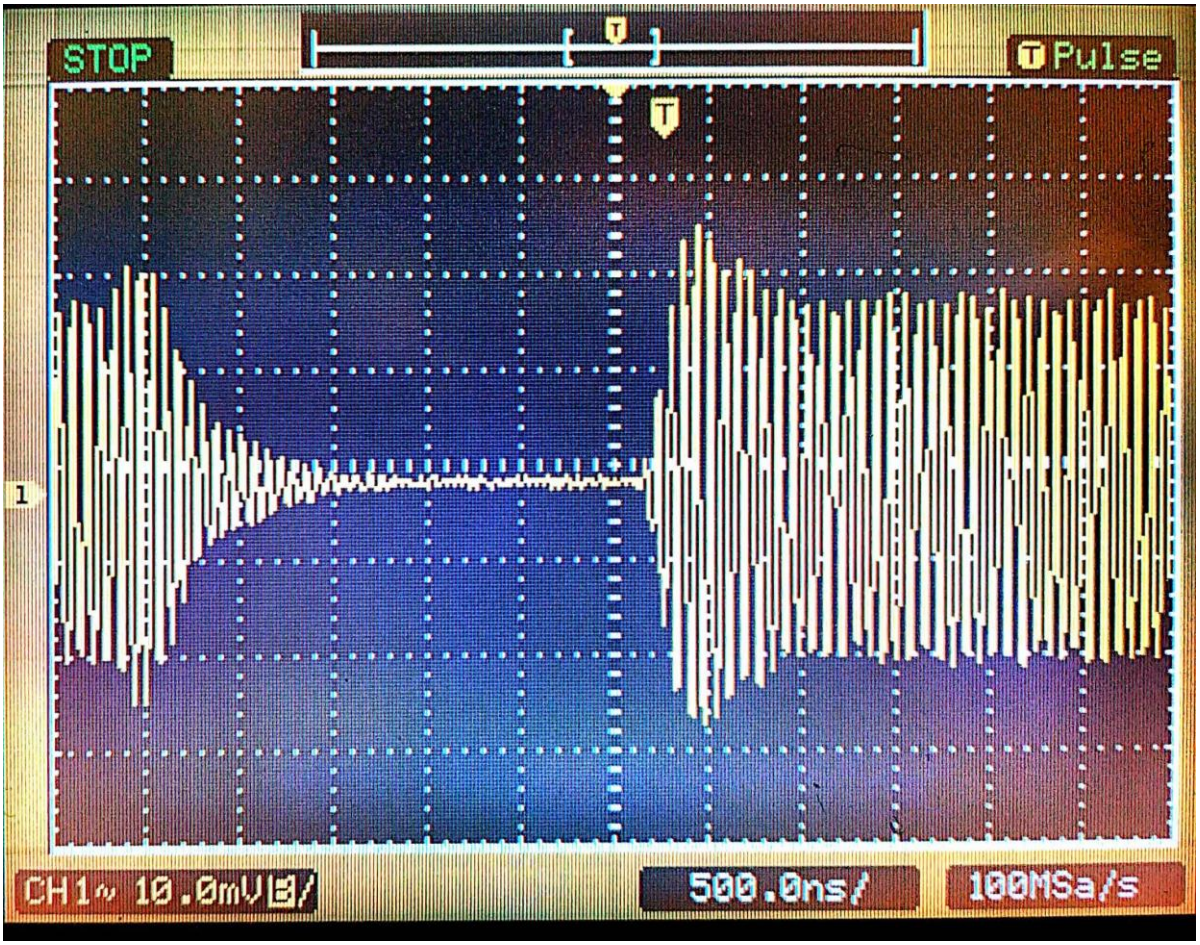
Στο παρόν κεφάλαιο θα εξεταστούν και θα αναλυθούν κάποιες ενδείξεις οι οποίες αποτελούν σημεία-σταθμούς για την εξέλιξη των πειραμάτων και τα τελικά συμπεράσματα.

Όπως έχει αναλυθεί και σε προηγούμενο κεφάλαιο, για να μπορέσουμε να κατανοήσουμε αν το σήμα που παρατηρείται στην οθόνη του παλμογράφου υποδηλώνει επικοινωνία από το PCD προς το PICC ή από το PICC στο PCD, πρέπει να λαμβάνουμε υπόψη τις μεθόδους modulation αλλά και encoding που ακολουθεί η κάθε μορφή επικοινωνίας. Αρχικά, επιβεβαιώσαμε πειραματικά πως η συχνότητα του φορέα είναι fc = 13,56MHz (Σχήμα 6.4).



Σχήμα 6.4: Συχνότητα Φορέα

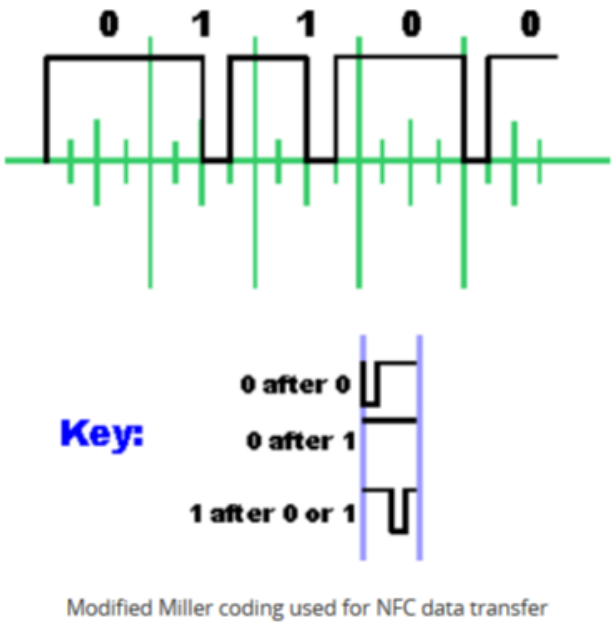
Σχετικά με τη διαμόρφωση, από τη θεωρία γνωρίζουμε πως χρησιμοποιείται 100% ASK modulation. Με αυτόν τον τρόπο, έχουμε λογικό «0» όταν η περιβάλλουσα του σήματος είναι 0 και λογικό «1» όταν η περιβάλλουσα του σήματος βρίσκεται στο μέγιστό της (100% βάθος διαμόρφωσης). Στο ακόλουθο σχήμα (Σχήμα 6.5) φαίνεται η διαμόρφωση του downlink καναλιού όπως καταγράφηκε από τον παλμογράφο.



Σχήμα 6.5: ένας 100% ASK παλμός που συμβαίνει στην αρχή της επικοινωνίας από το PCD στο PICC

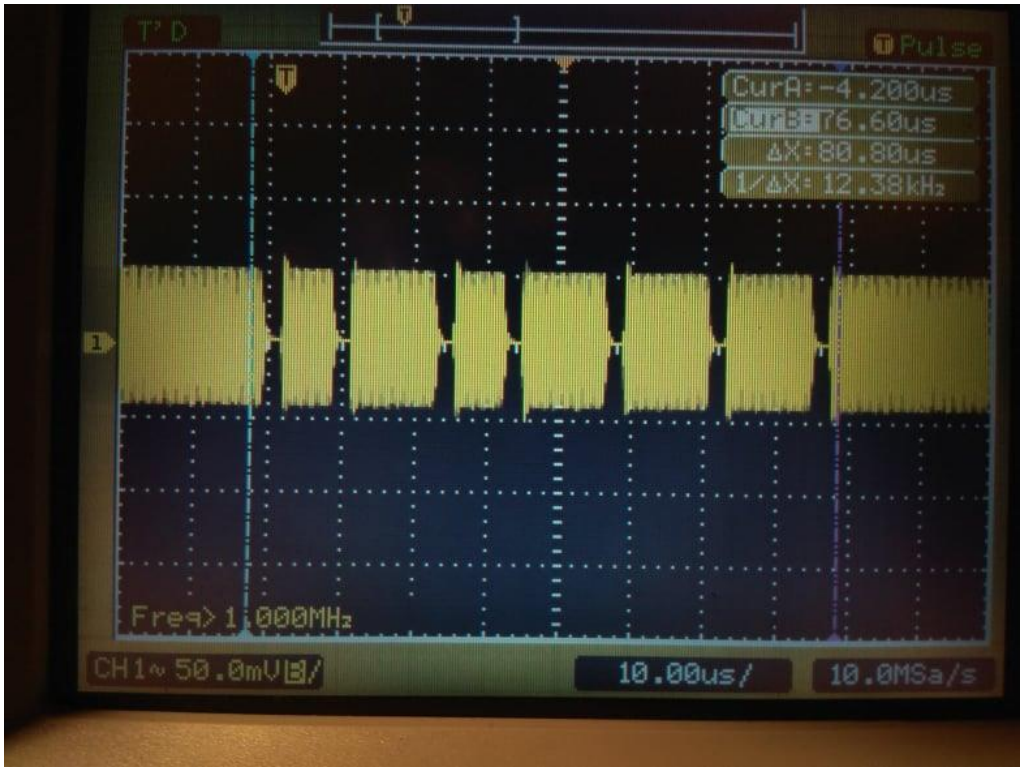
Είδαμε λοιπόν, πως το σύστημα αναπαριστά τις δύο στάθμες του ψηφιακού σήματος. Ωστόσο, για να αποκτήσει λογική ως ακολουθία θα πρέπει να συνυπολογιστεί το σχήμα κωδικοποίησης που εφαρμόζεται. Για την επικοινωνία του PCD προς το PICC χρησιμοποιείται κωδικοποίηση Modified Miller.

Η κωδικοποίηση Modified Miller χαρακτηρίζεται από τις παύσεις του φέροντος σήματος σε διαφορετικές θέσεις μιας περιόδου. Ανάλογα με την πληροφορία που μεταδίδεται, το λογικό bit ‘1’ κωδικοποιείται πάντα με τον ίδιο τρόπο, αλλά το λογικό bit ‘0’ κωδικοποιείται διαφορετικά, ανάλογα με το τι ακολουθεί.



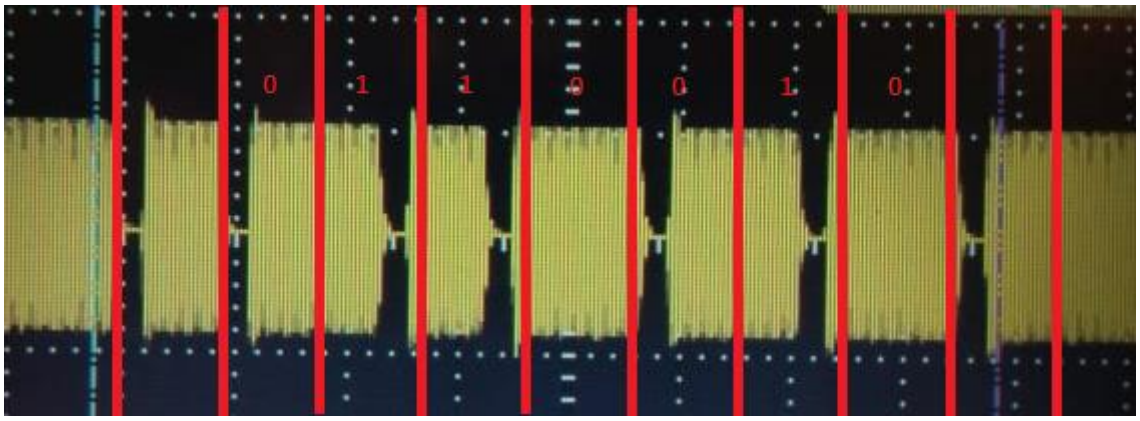
Σχήμα 6.6: Modified Miller encoding

Η πρώτη ακολουθία που πληροί τα χαρακτηριστικά που περιγράφονται παραπάνω, είναι η πρώτη εντολή που αποστέλλει το PCD στο PICC και φαίνεται στο Σχήμα 6.7 που ακολουθεί.



Σχήμα 6.7: Απεικόνιση πρώτης εντολής στο downlink κανάλι

Γνωρίζοντας το σχήμα κωδικοποίησης και το ότι η διάρκεια ενός bit είναι 9 μs (πιο συγκεκριμένα 9,44 μs) και πως οι εντολές ξεκινούν και τελειώνουν με λογικό «0», μπορούμε να ξεκινήσουμε την αποκωδικοποίηση της εντολής.



Σχήμα 6.8: Εντολή REQA με ανάλυση των bits

Από το παραπάνω σχήμα φαίνεται πως η ακολουθία αντιστοιχεί στο 0110010 αφού αποστέλλεται πρώτα το less significant bit.

Γνωρίζουμε από το πρότυπο πως οι πρώτες εντολές για την αρχικοποίηση της επικοινωνίας ξεκινούν από την μεριά του PCD. Το PCD πρακτικά αναζητεί PICCs εντός της εμβέλειάς του και αυτό γίνεται με τη χρήση της REQA εντολής.

b7	b6	b5	b4	b3	b2	b1	Meaning
1	0	1	0	0	1	0	WUPA
0	1	0	0	1	1	0	REQA

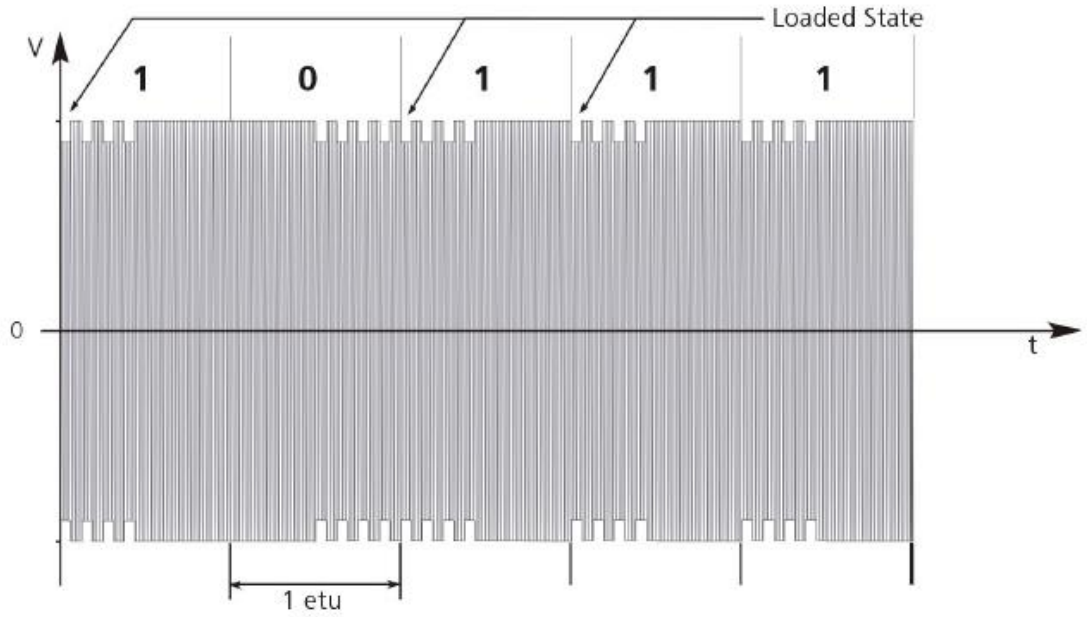
Σχήμα 6.9: Κωδικοποίηση των εντολών WUPA και REQA

Βάσει της θεωρίας, γνωρίζουμε πως η REQA εντολή αποτελείται από εννιά (9) bits. Συγκεκριμένα ξεκινά και τερματίζει με ένα λογικό 0 (start of logic 0, end of logic 0) και το βασικό της μέρος είναι εφτά (7) bits με τη σειρά 0110010.

Επομένως, στο Σχήμα 6.8 έχουμε αναγνωρίσει επιτυχώς την εντολή REQA. Ο εντοπισμός άλλων εντολών του command set μπορεί να πραγματοποιηθεί με αντίστοιχη μεθοδολογία.

Όσον αφορά την επικοινωνία από το PICC στο PCD, δηλαδή το uplink κανάλι, γνωρίζουμε πως εφαρμόζεται On Off keying Load Modulation και έτσι το λογικό «0» αναπαρίσταται με χαμηλό πλάτος της περιβάλλουσας καθώς υπάρχει φορτίο σε σειρά με την κεραία ενώ το λογικό «1» με μεγάλο πλάτος καθώς δεν υπάρχει φορτίο στην κεραία.

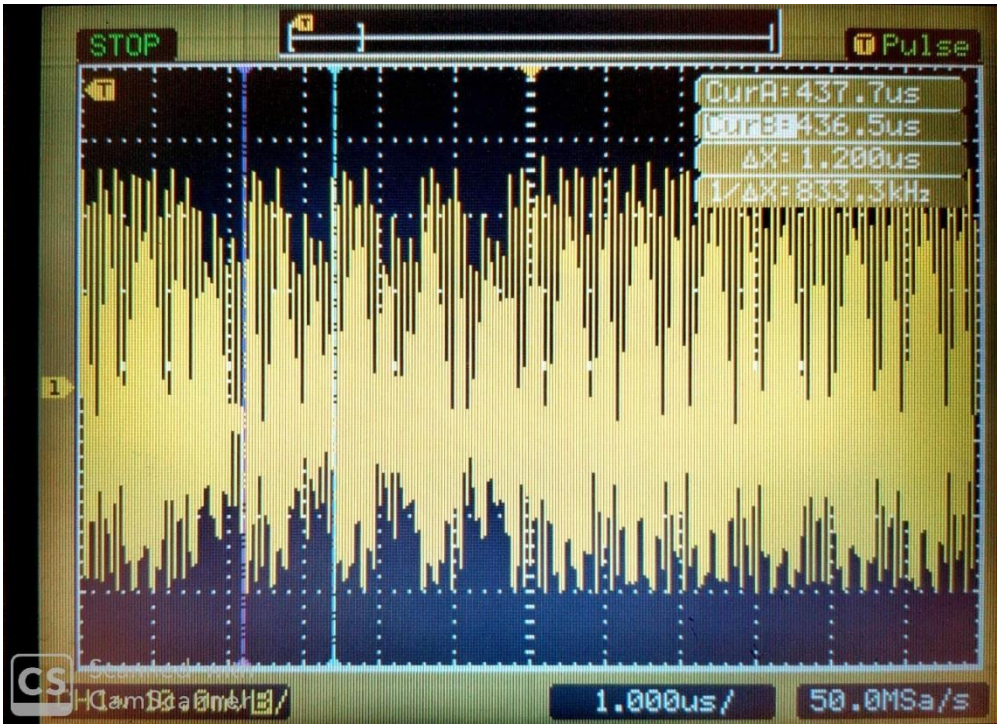
Η κωδικοποίηση που χρησιμοποιείται είναι Manchester και φαίνεται παρακάτω (Σχήμα 6.10). Ο υπο-φορέας στο uplink κανάλι είναι fsc = fc / 16 ≈ 847kHz.



Σχήμα 6.10: Manchester Encoding

Δυστυχώς αντίθετα από την περίπτωση του downlink καναλιού, εδώ δεν μπορέσαμε να εντοπίσουμε και να ταυτοποιήσουμε μια ολόκληρη εντολή καθώς με το υπάρχοντα εξοπλισμό δεν μπορέσαμε να ξεπεράσουμε δυσκολίες που είχαν να κάνουν με την έλλειψη συγχρονισμού.

Στην παρακάτω εικόνα (Σχήμα 6.11) φαίνεται καθαρά το βάθος της διαμόρφωσης, η συχνότητα του υπο-φορέα καθώς και ένα bit με τιμή 1.



Σχήμα 6.11: Uplink κανάλι επικοινωνίας

6.1.5 ΣΥΜΠΕΡΑΣΜΑΤΑ

Σε αυτό το σημείο αξίζει να σημειωθούν ορισμένα συμπεράσματα τα οποία προέκυψαν κατά τη διεξαγωγή του πειράματός μας. Καταφέραμε επιτυχώς να «ακούσουμε» και τα δύο κανάλια επικοινωνίας. Στην περίπτωση του downlink αναγνωρίσαμε μια ολόκληρη εντολή, ενώ στην περίπτωση του uplink μερικά μόνο bit.

Έτσι λοιπόν προκύπτει πως οποιοσδήποτε κακόβουλος με κατάλληλο εξοπλισμό στη διάθεσή του αλλά και με επαρκή γνώση του πρωτοκόλλου, δύναται να υποκλέψει ολόκληρη τη μη κρυπτογραφημένη επικοινωνία μεταξύ PCD και PICC. Το κανάλι επικοινωνίας από μόνο του δεν μπορεί να θεωρηθεί ασφαλές. Φυσικά, στην παρούσα εργασία δεν εξετάζεται η κρυπτογράφηση που εφαρμόζεται σε αυτού του είδους την επικοινωνία.

Σχετικά με την απόσταση: παρατηρήθηκε πως η απόσταση λειτουργίας διαφέρει από την απόσταση υποκλοπής, ή αλλιώς την απόσταση στην οποία μπορεί να βρίσκεται ο κακόβουλος «ωτακουστής» με τον εξοπλισμό του. Με τον εξοπλισμό που βρισκόταν στη διάθεσή μας, είχαμε τη δυνατότητα καταγραφής σήματος από το POS προς την κάρτα, στα σαράντα (40) cm ενώ η τυπική απόσταση λειτουργίας είναι κοντά στα 10cm. Όπως γίνεται κατανοητό, σε περίπτωση που διαθέτει κανείς καλύτερο εξοπλισμό, η συγκεκριμένη απόσταση θα ήταν ακόμα μεγαλύτερη.

6.2 JAMMING ΜΕ ΤΗ ΧΡΗΣΗ ΑΥΤΟΣΧΕΔΙΑΣ ΚΕΡΑΙΑΣ

Στο παρόν υποκεφάλαιο θα παρουσιαστεί η δεύτερη πειραματική προσπάθεια που έλαβε χώρα και αφορά στην προσπάθεια jamming με χρήση γεννήτριας και της αυτοσχέδιας κεραίας του προηγούμενου πειράματος.

Με τον όρο παρεμβολέας ή Radio Frequency (RF) Jammer αναφερόμαστε σε μία συσκευή η οποία μπορεί να χρησιμοποιηθεί ώστε να διαταράξει ή να εμποδίσει την επικοινωνία μέσω της μετάδοσης ενός ηλεκτρομαγνητικού σήματος (RF signal).

6.2.1 ΣΚΟΠΟΣ ΠΕΙΡΑΜΑΤΟΣ

Σκοπός της διεξαγωγής του συγκεκριμένου πειράματος είναι να αποδείξουμε πως κάποιος κακόβουλος, με τη χρήση σχετικά απλού εξοπλισμού, δύναται να προκαλέσει επίθεση τύπου άρνησης υπηρεσιών αποτρέποντας την επικοινωνία μεταξύ PCD και PICC.

6.2.2 ΕΞΟΠΛΙΣΜΟΣ ΠΕΙΡΑΜΑΤΟΣ

Για τη διεξαγωγή του πειράματος χρησιμοποιήθηκε μία γεννήτρια Rigol DG1022 (20 MHz). Στη γεννήτρια συνδέθηκε μία αυτοσχέδια κεραία, συγκεκριμένα χρησιμοποιήθηκε η ετικέτα MIFARE του προηγούμενου πειράματος. Έγιναν δυο δοκιμές: η πρώτη με στόχο ένα ζευγάρι PCD-PICC τεχνολογίας NFC και ένα ζευγάρι RFID. Ο αναγνώστης NFC που χρησιμοποιήθηκε σε αυτό το πείραμα ήταν ένα test EFT/POS. Επίσης χρησιμοποιήθηκε μία test πιστωτική/χρεωστική κάρτα. Ο RFID αναγνώστης που χρησιμοποιήθηκε ήταν το RFID reader MFRC522.

6.2.3 ΜΕΘΟΔΟΣ ΠΕΙΡΑΜΑΤΟΣ

Στο πείραμα αυτό, προσπαθήσαμε να επιτύχουμε τη διακοπή της επικοινωνίας PCD με PICC μέσω της παρεμβολής ενός ισχυρότερου ηλεκτρομαγνητικού σήματος, από εκείνο το οποίο εκπέμπει το PCD. Για να πετύχουμε παρεμβολή πρέπει να εκπέμψουμε στην συχνότητα του φορέα του σήματος, στη δική μας περίπτωση δηλαδή στα 13,56 MHz. Στην ιδανική περίπτωση θέλουμε ένα πολύ ισχυρό σήμα επομένως με τον απλό μας εξοπλισμό θα πρέπει να πλησιάσουμε πολύ κοντά στο τερματικό για να υπάρχει το οποιοδήποτε αποτέλεσμα.

Όσο αφορά την πρώτη δοκιμή με στόχο το ζευγάρι PCD-PICC NFC η προσπάθεια μας απέτυχε, παρόλο που δοκιμάστηκε από διάφορες αποστάσεις. Η αυτοσχέδια κεραία τοποθετήθηκε ακόμα και σε θέση στην οποία σχεδόν να εφάπτεται στο PICC, χωρίς όμως να υπάρξει κάποιο αποτέλεσμα.

Η δεύτερη δοκιμή μας όμως ήταν επιτυχής, όταν με τον ίδιο ακριβώς εξοπλισμό επιχειρήθηκε παρεμβολή της επικοινωνίας μεταξύ του RFID αναγνώστη και της ετικέτας. Συγκεκριμένα όταν πλησιάσαμε την αυτοσχέδια κεραία πολύ κοντά, σε απόσταση περίπου 7 εκατοστών από το RFID tag η ανάγνωση των δεδομένων από την κάρτα σταμάτησε και ξεκίνησε πάλι μόνο όταν απομακρύναμε την κεραία μας.

Σχήμα 6.12: Γεννήτρια και κεραία που χρησιμοποιήθηκαν για τη διεξαγωγή του πειράματος

6.2.4 ΣΥΜΠΕΡΑΣΜΑΤΑ

Η επικρατέστερη εξήγηση που μπορεί να δοθεί είναι πως πιθανώς η RFID επικοινωνία είχε πιο ασθενές σήμα και για αυτό καταφέραμε να τη διακόψουμε ενώ η προσπάθεια με τα PCD-PICC

(EFT POS συσκευή και πιστωτική κάρτα) να απέτυχε λόγω δυνατότερης εκπομπής του ηλεκτρομαγνητικού σήματος από αυτή της αυτοσχέδιας κεραίας που χρησιμοποιήσαμε στο πείραμα. Φυσικά πρέπει να υπογραμμίσουμε πως με καταλληλότερο εξοπλισμό μια τέτοια επίθεση θα μπορούσε να έχει αποτέλεσμα.

Γενικότερα όμως μια τέτοια επίθεση είναι αρκετά δύσκολο να γίνει στη πράξη και αυτό καθώς η εγγύτητα της συναλλαγής εξασφαλίζει πολύ ισχυρή επικοινωνία ανάμεσα στο PCD και PICC, επομένως ένας κακόβουλος θα έπρεπε να πλησιάσει τον παρεμβολέα πάρα πολύ κοντά για να έχει επιτυχία.

ΚΕΦΑΛΑΙΟ 7^{ο} – ΠΡΟΤΑΣΕΙΣ

Η προστασία των τραπεζικών λογαριασμών και των οικονομικών συναλλαγών απασχολεί όλους τους καταναλωτές δίχως καμία αμφιβολία. Αποτελεί ένα ιδιαίτερα ευαίσθητο ζήτημα και δεδομένης της εξέλιξης της τεχνολογίας, ήδη τα μέτρα προστασίας που έχουν ληφθεί σε λογισμικό αλλά και υλικό, είναι σημαντικά. Οι κακόβουλες επιθέσεις όμως, εξελίσσονται συνεχώς. Οι υπεύθυνοι χρηματοπιστωτικοί οργανισμοί καλούνται να βρίσκονται πάντα ένα βήμα μπροστά ώστε να εξασφαλίζουν την εμπιστοσύνη και των πελατών. Παρακάτω θα παρουσιαστούν/σχολιαστούν κάποιες προτάσεις σε λογισμικό αλλά και υλικό επίπεδο. Ορισμένες είναι ήδη διαθέσιμες στους καταναλωτές αλλά όχι ευρέως χρησιμοποιούμενες.

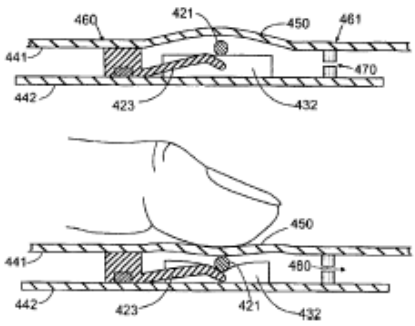
7.1 HARDWARE

Ενώ υπάρχουν πολλές ιδέες για την απενεργοποίηση της ασύρματης διεπαφής των έξυπνων καρτών, οι περισσότερες έξυπνες κάρτες με ανέπαφη διασύνδεση και dual interface, δε διαθέτουν τέτοιους μηχανισμούς.

Ακολουθεί αξιολόγηση τριών προσεγγίσεων για την εφαρμογή καρτών με μια ασύρματη διασύνδεση που μπορεί να ενεργοποιηθεί/απενεργοποιηθεί από τον ίδιο το χρήστη ανάλογα με τη χρήση που θέλει να πραγματοποιήσει.

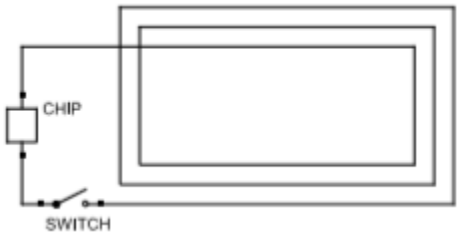
Αποκοπή της κεραίας με τη χρήση διακόπτη

Ένα κουμπί μπορεί να ενσωματωθεί στην κεραία μιας ανέπαφης κάρτας, ώστε η τελευταία να είναι αποσυνδεδεμένη, εκτός εάν ο χρήστης πιέσει το κουμπί. Συγκεκριμένα, ένας διακόπτης (κανονικά ανοικτός) προστίθεται σε σειρά στην κεραία.



Σχήμα 7.1: Αποκοπή της κεραίας με χρήση διακόπτη

Όταν ο χρήστης θέλει να δώσει πρόσβαση στην ασύρματη διεπαφή, ο διακόπτης είναι κλειστός και συνδέει την κεραία με τον ενσωματωμένο μικροεπεξεργαστή (chip) της έξυπνης κάρτας.



Σχήμα 7.2: Αποκοπή της κεραίας με χρήση διακόπτη

Εναλλακτικά έχει μελετηθεί η τοποθέτηση ενός διακόπτη παράλληλα της κεραίας. Σε αυτό το σενάριο, ο διακόπτης θα είναι κανονικά κλειστός, οπότε θα βραχυκυκλώνει στα άκρα του chip και δε θα διαρρέεται ρεύμα μέσα από αυτό. Όταν ο χρήστης θέλει να ενεργοποιήσει την ασύρματη διεπαφή, ο διακόπτης ανοίγει ώστε να επιτρέψει στο σήμα από την κεραία να περάσει στο chip.

Μια άλλη προσέγγιση είναι ο έλεγχος της κεραίας να γίνεται με κάποιον ηλεκτρονικό διακόπτη *(transistor)* ώστε να μην είναι απαραίτητη η φυσική επαφή αλλά να μπορεί αυτός να ελεγχθεί και με άλλο τρόπο.[17]

7.2 ΠΡΟΤΑΣΕΙΣ ΣΕ ΕΠΙΠΕΔΟ ΛΟΓΙΣΜΙΚΟΥ

Μια ακόμα επιλογή που αξίζει να εξεταστεί αποτελεί η διαχείριση της κάρτας μέσω κάποιας εφαρμογής, εγκατεστημένης σε έξυπνη συσκευή. Ο χρήστης μπορεί να επιλέξει ποιες εφαρμογές θα είναι διαθέσιμες στην ανέπαφη διεπαφή.

Πλέον η πλειοψηφία των χρηματοπιστωτικών οργανισμών διαθέτουν εφαρμογές για τη διαχείριση των χρεωστικών/πιστωτικών καρτών των πελατών τους. Συνεχώς προστίθενται νέες δυνατότητες διαχείρισης στη χρήση αυτών. Παρακάτω περιγράφονται μερικές προτάσεις σχετικά με τη διαχείριση των καρτών σε επίπεδο λογισμικού.

Ασφάλεια τοποθεσίας

Με την ενεργοποίηση αυτής της λειτουργίας στην εφαρμογή, μπορεί να χρησιμοποιηθεί η θέση GPS της κινητής συσκευής. Με αυτόν τον τρόπο, εάν κάποιος κακόβουλος έχει υποκλέψει την κάρτα είτε τα στοιχεία αυτής και προσπαθήσει να τη χρησιμοποιήσει σε κάποια άλλη περιοχή θα αποτραπεί η πραγματοποίηση της συναλλαγής.

Πληρωμές Magstripe

Η δυνατότητα απενεργοποίησης των πληρωμών με τη χρήση της μαγνητικής λωρίδας θα βοηθήσει στην αποφυγή της χρήσης της κάρτας με σκοπό το δόλο ή την κλωνοποίηση. Είναι γνωστή, όπως έχει αναφερθεί και εκτενέστερα σε παραπάνω κεφάλαια, η έλλειψη ασφάλειας στις συναλλαγές όπου χρησιμοποιείται η μαγνητική λωρίδα. Αδιαμφισβήτητα, προτείνεται η χρήση της μεθόδου Chip και PIN όποτε αυτή είναι διαθέσιμη.

Πληρωμές χωρίς επαφή

Μια ακόμα λειτουργία που προτείνεται είναι η δυνατότητα απενεργοποίησης των ανέπαφων συναλλαγών όποτε ο καταναλωτής δεν πρόκειται να κάνει σχετική χρήση.

Αναλήψεις ATM

Χρήσιμη είναι και η δυνατότητα απενεργοποίησης των αναλήψεων μέσω ATM. Σε περίπτωση υποκλοπής της κάρτας και εάν ο κακόβουλος γνωρίσει τον κωδικό PIN, με αυτή τη λειτουργία θα εμποδιστεί οποιαδήποτε ενέργεια.

Συναλλαγές ηλεκτρονικού εμπορίου

Μία από τις πιο συνηθισμένες προσπάθειες των κακόβουλων αποτελεί η υποκλοπή των στοιχείων των καρτών με σκοπό τη χρήση τους σε αγορές κ.α. . Η απενεργοποίηση των συναλλαγών ηλεκτρονικού εμπορίου θα αποτρέψει την ολοκλήρωση κακόβουλων πληρωμών online.

Φυσικά, δεν πρέπει να παραλείπονται οι συνεχείς ειδοποιήσεις μέσω της εφαρμογής, είτε μέσω ηλεκτρονικών μηνυμάτων ή SMS, με τις οποίες ο κάτοχος της κάρτας να ενημερώνεται για οποιαδήποτε ύποπτη κίνηση και να προχωράει στις ανάλογες ενέργειες.[16]

ΚΕΦΑΛΑΙΟ 8ο – ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Σωτήρης Συμαρκέζης, Internet Banking
https://www.hba.gr/5Ekdosis/UplPDFs/deltia/3_2003/27-40.pdf

[2] Ανέπαφες συναλλαγές με τις κάρτες της Τράπεζας Πειραιώς
https://www.piraeusbank.gr/el/idiwtes/kartes/anepafes-sinallages

[3] https://www.reader.gr/news/oikonomia/mastercard-exaplonontai-ragdaia-oi-anepafes-synallages-stin-ellada

[4] Αρχή Προστασίας Προσωπικού Χαρακτήρα – Απόφαση Αρ. 48/2018

[5] Igoe, Tom, Don Coleman, and Brian Jepson. Beginning NFC: near field communication with Arduino, Android, and Phonegap. " O'Reilly Media, Inc.", 2014.

[6] RAJARAJAN, S., KS SURESH, and M. PRABHU. "INTEGRATED DEBIT CUM CREDIT CARD WITH DYNAMIC CARD SELECTION AND CARD LOCKING." Journal of Theoretical & Applied Information Technology 58.3 (2013).

[7] Santosh Khadsare, Smart Cards

https://www.slideshare.net/santoshkhadsare/smart-card

[8] Hoffmann, Max. "Hardware Supported Man-in-the-Middle Attack Interfering with Smartcard Communication Protocols."

[9] Mayes, Keith E., and Konstantinos Markantonakis, eds. Smart cards, tokens, security and applications. Vol. 2. No. 3. New York: Springer, 2008.

[10] Salvador Mendoza, Intro to Analyze NFC Payment Methods and Contactless Cards
https://salmg.net/2017/09/12/intro-to-analyze-nfc-contactless-cards/

[11] EMVCo - EMV Contactless Book A, Architecture and General Requirements v 2.4

[12] RAJARAJAN, S., KS SURESH, and M. PRABHU. "INTEGRATED DEBIT CUM CREDIT CARD WITH DYNAMIC CARD SELECTION AND CARD LOCKING." Journal of Theoretical & Applied Information Technology 58.3 (2013).

[13] McBride, Brendan, Nigel McKelvey, and Kevin Curran. "Security issues with contactless bank cards." Journal of Information 1.3 (2015): 53-58.

[14] EMVco - A Guide to EMV Chip Technology Version 2.0 November 2014

[15] Markantonakis, Konstantinos, et al. "Attacking smart card systems: Theory and practice." information security technical report 14.2 (2009): 46-56.

[16] Revolut, Enabling Security Settings
https://www.revolut.com/help/exploring-revolut/managing-my-money/enabling-security-settings

[17] Roland, Michael, and Michael Hölzl. "Evaluation of Contactless Smartcard Antennas." arXiv preprint arXiv:1507.06427 (2015).

[18] MF0ICU2, MIFARE Ultralight C, Rev. 30, Product short data sheet

[19] MIFARE Type Identification Procedure
https://www.nxp.com/docs/en/application-note/AN10833.pdf

[20] Texas Instruments – ISO/NFC Standards and Specifications Overview (NFC/RFID Trainign Module #1 (2014) S2 MCU NFC/RFID Applications Team)

ΠΙΝΑΚΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

Συντομογραφία	**Περιγραφή**
AAC	Application Authentication Cryptogram
APDU	Application Protocol Data Unit
ARPC	Authorization Response Cryptogram
ARQC	Authorisation Request Cryptogram
ASK	Amplitude Shift Keying
ATC	Application Transaction Counter
ATM	Automated Teller Machine
CID	Card Identifier
CVM	Cardholder Verification Method
DoS	Denial of Service
EEPROM	Electrically Erasable Programmable Read Only Memory
EFT/POS	Electronic Funds Transfer/Point of Sales
EMVCo	Europay, Mastercard, Visa Companies. EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo is currently owned by American Express, JCB, MasterCard and Visa
ICC	Integrated Circuit Card
IIN	Issuer Identification Number
ISO	International Organization for Standardization
MII	Major Industry Identifier
MMU	Memory Management Unit
NFC-A	Near Field Communication – NFC-A Technology
NFC-B	Near Field Communication – NFC-B Technology
PCD	Proximity Coupling Device (Reader)
PICC	Proximity Integrated Circuit Card
RFID	Radio Frequency Identification
SAK	Select Acknowledge
SIM	Subscriber Identity Modules
TC	Transaction Certificate
UID	Unique Identifier