ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μ.Π.Σ. ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

APPLE PAY - ΑΞΙΟΛΟΓΗΣΗ ΥΠΗΡΕΣΙΑΣ ΚΑΙ ΑΠΟΤΙΜΗΣΗ ΑΣΦΑΛΕΙΑΣ

ΠΑΠΑΔΟΠΟΥΛΟΣ ΜΩΥΣΗΣ

ΕΠΙΒΛΕΠΩΝ:

Δρ. ΛΑΜΠΡΙΝΟΥΔΑΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΠΕΙΡΑΙΑΣ, ΙΟΥΛΙΟΣ 2015

Περίληψη

Η ραγδαία ανάπτυξη που παρουσίασε τα τελευταία χρόνια η αγορά των έξυπνών συσκευών σε συνδυασμό με τον ολοένα αυξανόμενο όγκο των συναλλαγών που πραγματοποιούνται ηλεκτρονικά, οδήγησε πολλές από τις εταιρίες που δραστηριοποιούνται στον χώρο της τεχνολογίας να θελήσουν να αποκτήσουν μερίδιο της αγοράς. Την αρχή έκαναν οι κατασκευαστές των έξυπνων συσκευών, οι οποίοι ενσωμάτωσαν την τεχνολογία NFC στις συσκευές τους, μαζί με τους παρόχους κινητής τηλεφωνίας όπου ενσωμάτωσαν το απαραίτητο Secure Element στις SIM κάρτες τους και φυσικά των τραπεζών. Το μοντέλο αυτό δεν υπήρξε πολύ πετυχημένο λόγω της προσπάθειας που έκανε το κάθε μέρος προκειμένου να αποκτήσει ισχυρότερη θέση.

Σύντομα έγινε αντιληπτό ότι το μοντέλο πρέπει να αλλάξει με τη συμμετοχή όσο το δυνατόν λιγότερων εμπλεκόμενων μερών. Η αρχή έγινε από την Google, η οποία παρουσίασε το Google Wallet, όπου τα στοιχεία των καρτών αποθηκεύοντας είτε στο Secure Element του NFC chip είτε στο cloud. Την μεγάλη όμως διαφορά την έκανε η Apple με την παρουσίαση της υπηρεσίας Apple Pay υιοθετώντας τη τεχνολογία του NFC, από την οποία κρατούσε αποστάσεις μέχρι εκείνη τη στιγμή, και εφαρμόζοντας παράλληλα το framework του tokenisation που μόλις μερικούς μήνες πριν είχε διαθέσει το EMVCo.

Το νέο στοιχείο του Apple Pay είναι ότι δεν αποθηκεύει σε κανένα σημείο τον πραγματικό αριθμός της κάρτας αλλά αντιθέτως παράγεται και αποθηκεύεται αποκλειστικά και μόνο στο Secure Element της συσκευής το λεγόμενο Device Account Number σύμφωνα με την Apple, ή το payment token κατά την ορολογία του EMVCo. Το Device Account Number αντικαθιστά τον πραγματικό αριθμό της κάρτας αλλά είναι παράλληλα απόλυτα συσχετισμένο με αυτό.

Η ασφάλεια που προσφέρει η συγκεκριμένη υλοποίηση είναι αρκετά σημαντική αφού πλέον δεν χρησιμοποιείται ο πραγματικός αριθμός της κάρτας και έτσι δεν μπορεί να υποκλαπεί. Ακόμα βέβαια και στην περίπτωση που τελικά υποκλαπεί το Device Account Number, αυτό από μόνο του δεν μπορεί να χρησιμοποιηθεί σε άλλα κανάλια.

Περιεχόμενα

Εισαγωγή 7
1. Tokenisation 9
1.1 Payment Token 10
1.1.1 Token Expiry Date 11
1.1.2 Last 4 Digits of PAN 11
1.1.3 PAN Product ID 11
1.1.4 POS Entry Mode 11
1.1.5 Token Request Indicator 11
1.1.6 Token Requestor ID 12
1.1.7 Token Assurance Level 12
1.1.8 Token Assurance Data 12
1.1.9 Token Cryptogram 12
1.2 Token Service Provider (TSP) 13
1.2.1 Provision Platform 13
1.2.2 Transaction Platform 14
2. Radio Frequency Identification 16
2.1 Αναγνώστες 16
2.2 Ετικέτες 17
2.2.1 Χωρητικότητα και υπολογιστική ικανότητα 18
2.2.2 Πηγή ενέργειας 19
2.3 Συχνότητα λειτουργίας 19
3. Near Field Communication 20
4. Secure Element 21
5. EMVCo 22
5.1 Επίπεδα Ασφάλειας 22
5.1.1 Card Authentication 23
5.1.2 Cardholder Verification 23
5.1.3 Transaction Authorization 24
5.2 Contactless 25
6. Apple Pay 26
6.1 Passbook 26
6.2 Touch ID 27
6.3 Skin Sensor 28

6.4 Find My iPhone....29
6.4.1 Εντοπισμός συσκευής....29
6.4.2 Αναπαραγωγή ήχου....29
6.4.3 Λειτουργία απώλειας....29
6.4.4 Σβήσιμο Συσκευής....30
6.5 Τρόπος λειτουργίας....30
6.5.1 Προσθήκη κάρτας....30
6.5.2 Εκτέλεση πληρωμών....31
6.5.3 Υποστηριζόμενες συσκευές....34
6.6 Ασφάλεια και Ιδιωτικότητα....34
6.7 Αδυναμίες....36
7. Διαφορετικές υλοποιήσεις....37
7.1 Android Pay....37
7.2 Samsung Pay....38
7.3 CurrentC....38
Συμπεράσματα....39
Βιβλιογραφία....41

Ευρετήριο Σχημάτων

Σχήμα 1: Tokenisation Ecosystem 9
Σχήμα 2: Provision Platform 14
Σχήμα 3: Transaction Platform 15
Σχήμα 4: Επικοινωνία host – αναγνώστη 17
Σχήμα 5: Επικοινωνία μεταξύ RFID αναγνώστη και RFID ετικετών 18
Σχήμα 6: Smart Card Layout 21
Σχήμα 7: Οι τρεις φάσεις ασφάλειας του EMV πρωτοκόλλου 22
Σχήμα 8: Προσθήκη κάρτας στο Apple Pay 31
Σχήμα 9: Apple Pay - In stores payments 32
Σχήμα 10: Apple Pay - In apps payments 33

Ευρετήριο Πινάκων

Πίνακας 1: Συχνότητες RFID 19
Πίνακας 2: Apple Pay - Συμβατές Συσκευές 34
Πίνακας 3: Συγκριτικά στοιχεία συστημάτων πληρωμών 37

Συντομογραφίες

ACH	Automated Clearing House
ATM	Automated Teller Machine
BIN	Bank Identification Number
BLE	Bluetooth Low Energy
CDA	Combined Data Authentication
CNP	Card Not Present
CVV	Card Verification Value
DAN	Device Account Number
DDA	Dynamic Data Authentication
EFT	Electronic Funds Transfer
eSE	embedded Secure Element
HCE	Host Card Emulation
MCX	Merchant Customer Exchange
MNO	Mobile Network Operator
NFC	Near Field Communication
PAN	Personal Account Number
PIN	Personal Identification Number
POS	Point Of Sales
RFID	Radio Frequency IDentification
SDA	Static Data Authentication
SE	Secure Element
SIM	Subscriber Identity Module
TSP	Token Service Provider

Εισαγωγή

Από τα μέσα του 20ου αιώνα κατά τον οποίο η ραγδαία αύξηση αγοράς καταναλωτικών αγαθών δημιούργησαν την ανάγκη χρήσης τραπεζικών (χρεωστικών/πιστωτικών) καρτών μέχρι και σήμερα που ο τρόπος απόκτησης των αγαθών έχει παντελώς αλλάξει, η βιομηχανία πληρωμών με χρήση τραπεζικής κάρτας προσπαθεί να προσαρμοστεί με τις εκάστοτε ανάγκες. Η πρώτη τραπεζική κάρτα η οποία ονομαζόταν “Charge-it” εκδόθηκε το 1946 από έναν τραπεζίτη στο Μπρούκλιν και ήταν μια κλειστού τύπου κάρτα όπου όταν ο πελάτης την χρησιμοποιούσε για την αγορά αγαθών, ο λογαριασμός του προωθούνταν στην τράπεζα, η οποία πλήρωνε τον πωλητή και τραβούσε τα χρήματα από τον λογαριασμό του κατόχου. Όλες οι κάρτες μέχρι και το 1966 ακολουθούσαν το ίδιο μοντέλο κλειστού κυκλώματος, όπου μια κάρτα μπορούσε να χρησιμοποιηθεί αποκλειστικά από τους πελάτες των εκδοτριών τραπεζών και μόνο στους συνεργαζόμενους εμπόρους των συγκεκριμένων τραπεζών.

Η πρώτη εμφάνιση τραπεζικής κάρτας γενικής χρήσης ήταν το 1966 όταν η Bank of America ίδρυσε την BankAmerica Service Corporation, η οποία αργότερα έγινε γνωστή ως VISA. Οι κάρτες αυτές είναι οι γνωστές μέχρι και σήμερα πλαστικές κάρτες με την μαγνητική ταινία στο πίσω μέρος, στην οποία είναι αποθηκευμένα τα στοιχεία εκείνα που απαιτούνται για την εκτέλεση μιας ηλεκτρονικής συναλλαγής. Η μαγνητική ταινία δεν διαθέτει κανένα επίπεδο ασφάλειας δεδομένου ότι ο οποιοσδήποτε με πολύ απλά και φτηνά τεχνικά μέσα μπορεί να διαβάσει, να μεταβάλει η ακόμα και να αντιγράψει μια κάρτα.

Η πρώτη σοβαρή προσπάθεια για την εισαγωγή ισχυρών μέσων προστασίας ξεκίνησε το 1994 από τους οργανισμούς Europay, MasterCard και Visa, οι οποίοι εργάστηκαν από κοινού πάνω σε ένα έργο με σκοπό την εφαρμογή των έξυπνων καρτών, στις τραπεζικές κάρτες, με όλα τα χαρακτηριστικά που αυτές προσφέρουν στο οποίο και έδωσαν το όνομα EMV από τα αρχικά τους.

Υπήρξαν βέβαια και άλλες αλλαγές που υλοποιήθηκαν προσπαθώντας πάντα να ακολουθήσουν τις εξελίξεις της τεχνολογίας όπως ήταν η εφαρμογή του Radio Frequency Identification (RFID) με την χρήση των contactless καρτών αλλά και την υιοθέτηση του Near Field Communication (NFC) για υποστήριξη εκτέλεσης συναλλαγών μέσω έξυπνων συσκευών.

Παρόλο που το NFC υποστηρίχθηκε από πολύ μεγάλες εταιρίες που δραστηριοποιούνται στον χώρο της τεχνολογίας και οι προοπτικές ήταν και παραμένουν πολύ υψηλές, υπήρχε μια σημαντική απουσία και αυτή δεν ήταν άλλη από την Apple, η οποία ως γνωστόν

προσπαθεί πάντα να αναπτύσσει δικές της καινοτόμες υλοποιήσεις. Πράγματι μετά από μια μάλλον διερευνητική κίνηση με την τεχνολογία iBeacon, η οποία στηριζόταν ουσιαστικά στη τεχνολογία Bluetooth Low Energy (BLE), στις 09 Σεπτεμβρίου του 2014 κατά την διάρκεια της ετήσιας παρουσίασης για τα νέα προϊόντα της εταιρίας παρουσιάστηκε η υπηρεσία Apple Pay με τον τίτλο «Το πορτοφόλι σου. Χωρίς το πορτοφόλι.» και για πρώτη φορά η Apple υιοθετεί την χρήση της τεχνολογίας NFC.

Όπως ακριβώς αναφέρει και ο τίτλος του Apple Pay με αυτή την υπηρεσία μπορεί κανείς να πραγματοποιήσει ηλεκτρονικές πληρωμές χωρίς το πορτοφόλι του, χωρίς δηλαδή την παρουσία κατά την συναλλαγή μιας φυσικής κάρτας. Η συγκεκριμένη επομένως υλοποίηση στοχεύει στην αντικατάσταση των φυσικών καρτών από τις ίδιες τις συσκευές της Apple (iPhone, iPad, Apple Watch) τόσο για αγορές σε φυσικά καταστήματα όσο και μέσω των εφαρμογών.

Τι πραγματικά όμως είναι το Apple Pay; Είναι μια νέα τεχνολογία ή είναι μια νέα υπηρεσία η οποία συνδυάζει άλλες υπάρχουσες τεχνολογίες, πλαίσια (frameworks) και προδιαγραφές; Πως αλλάζει τον τρόπο χρήσης των τραπεζικών καρτών και τι επιπλέον επίπεδα ασφαλείας προσφέρει; Τελικά αυτός ο νέος τρόπος ηλεκτρικών πληρωμών μπορεί να εφαρμοστεί σε όλα τα κανάλια πώλησης; Τι γίνεται με τις πληρωμές χωρίς την παρουσία κάρτας (CNP) στις συναλλαγές του λεγόμενου eCommerce; Όλα αυτά τα ερωτήματα αποτελούν αντικείμενο της παρούσας εργασίας και αφού προηγηθεί, στις επόμενες ενότητες, μια περιγραφή όλων των τεχνολογιών και υπηρεσιών που εφαρμόζονται από την υπηρεσία Apple Pay, θα ακολουθήσει μια προσπάθεια συνολικής αξιολόγησης της υπηρεσίας και θα ολοκληρωθεί με την αποτίμηση της ασφάλειας που προσφέρει.

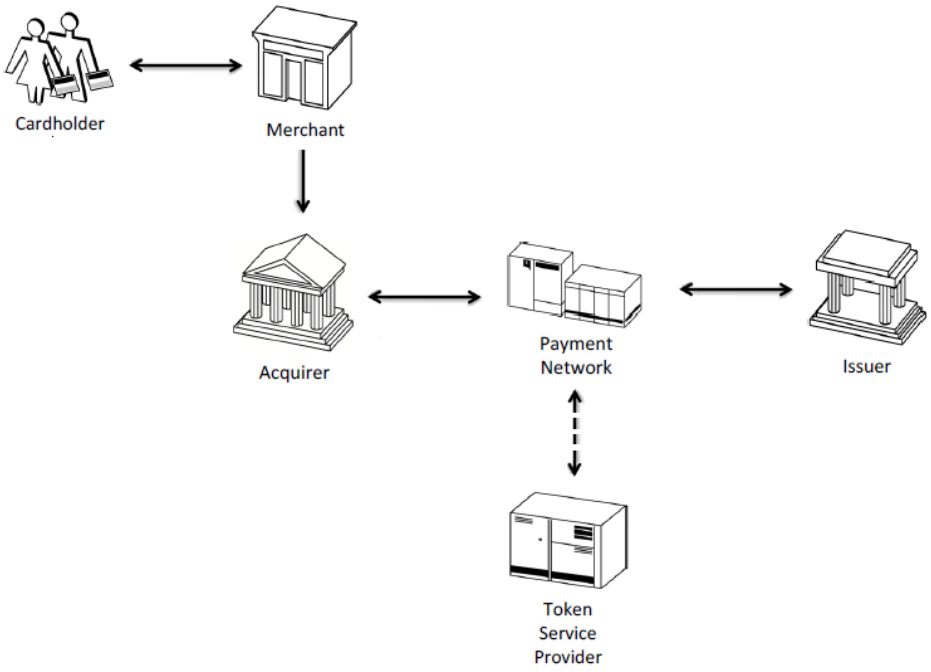
1. Tokenisation

Tokenisation είναι η διαδικασία αντικατάστασης του Personal Account Number (PAN), το οποίο διαθέτουν όλες οι πλαστικές τραπεζικές κάρτες (χρεωστικές και πιστωτικές), με έναν άλλον λογαριασμό χρήσης, ο οποίος ονομάζεται payment token και διατηρεί όλες τις απαραίτητες πληροφορίες αυξάνοντας όμως την ασφάλεια τόσο των συναλλαγών όσο και των κατόχων του.

Οι βασικές λειτουργίες του tokenization είναι [3]:

- Έκδοση και παροχή token
- Επεξεργασία συναλλαγών
- Διασυνδέσεις με άλλα συστήματα - Application Programming Interfaces (APIs)

Όπως γίνεται κατανοητό για την υλοποίηση των παραπάνω διαδικασιών καθίσταται αναγκαία η ύπαρξη ενός νέου παρόχου, ο οποίος θα είναι επιφορτισμένος με την εκτέλεση αυτών των υπηρεσιών και ονομάζεται Token Service Provider (TSP). Ο TSP μπορεί να υλοποιείται είτε από τους εκδότες των καρτών (τράπεζες), είτε από τους οργανισμούς των καρτών (Visa, MasterCard, AmEx κ.α.) ή ακόμα και από έναν τρίτο φορέα ο οποίος μπορεί να είναι τελείως ανεξάρτητος.



Σχήμα 1: Tokenisation Ecosystem

1.1 Payment Token

Payment token είναι ένας αριθμός ο οποίος αντικαθιστά το PAN μιας τραπεζικής κάρτας και χρησιμοποιείται κυρίως σε ηλεκτρονικές πληρωμές μέσω διαδικτύου για την προστασία του φυσικού αριθμού της κάρτας. Το payment token μπορεί να έχει οποιαδήποτε μορφή αλλά για λόγους συμβατότητας και διαλειτουργικότητας των συστημάτων, ακολουθείται η ίδια μορφή που χρησιμοποιείται και από το Personal Account Number (PAN) των τραπεζικών καρτών.

PAN είναι ο αριθμός λογαριασμού που διαθέτουν όλες οι τραπεζικές κάρτες σύμφωνα με το πρότυπο ISO/IEC 7812 και αποτελείται από 13 έως 19 ψηφία. Η δομή του PAN είναι η ακόλουθη [11]:

6 ψηφία:	Ένας μοναδικός αριθμός (BIN) ο οποίος εκχωρείται στην εκδότρια τράπεζα. Κάθε εκδότρια τράπεζα μπορεί να διαθέτει παραπάνω από ένα BIN.
6-12 ψηφία:	Το εύρος των αριθμών καρτών που μπορεί να χρησιμοποιηθεί στο δεδομένο BIN.
1 ψηφίο:	Είναι το ψηφίο επαλήθευσης (check digit) και υπολογίζεται με την χρήση του Luhn αλγορίθμου.

Τα payment tokens διαθέτουν ένα πλήθος από χαρακτηριστικά, μερικά από τα οποία είναι υποχρεωτικά, ορισμένα είναι υπό συνθήκη υποχρεωτικά, ενώ κάποια άλλα είναι προαιρετικά. Τα χαρακτηριστικά στοιχεία (elements) των payment tokens είναι τα ακόλουθα [3]:

- Token Expiry Date
- Last 4 Digits of PAN
- PAN Product ID
- POS Entry Mode
- Token Requestor ID
- Token Assurance Level
- Token Assurance Data
- Token Cryptogram
- Token Request Indicator

1.1.1 Token Expiry Date

Είναι η ημερομηνία λήξης του payment token, η οποία όμως είναι διαφορετική από την ημερομηνία λήξης της φυσικής κάρτας και μπορεί να έχει οποιαδήποτε διάρκεια, από μια ημέρα για τα δυναμικά tokens μέχρι και την ημερομηνία λήξης της φυσικής κάρτας για τα στατικά.

1.1.2 Last 4 Digits of PAN

Περιλαμβάνει τα 4 τελευταία ψηφία της φυσικής κάρτας και χρησιμοποιείται είτε ως ένα επιπλέον μέτρο επαλήθευσης του payment token με τον πραγματικό αριθμός της κάρτας, είτε για την εκτύπωση του στην απόδειξη της συναλλαγής στις υλοποιήσεις που αυτό απαιτείται.

1.1.3 PAN Product ID

Είναι ένα προαιρετικό στοιχείο, το οποίο περιέχει τον τύπο της φυσικής κάρτας και χρησιμοποιείτε σε υλοποιήσεις που εφαρμόζουν διαφορετικές πολιτικές χρέωσης ή προνομιών ανά τύπο κάρτας.

1.1.4 POS Entry Mode

Υποδεικνύει τον τρόπο χρήσης του payment token, επομένως ένα payment token μπορεί να χρησιμοποιηθεί μόνο από συγκεκριμένα κανάλια τα οποία σχετίζονται με την διαδικασία αίτησης για την έκδοσης του.

1.1.5 Token Request Indicator

Προαιρετικό πεδίο το οποίο αποστέλλεται ως δείκτης κατά τη διάρκεια μιας αίτησης για την έκδοση payment token προκειμένου να υποδείξει ότι το συγκεκριμένο μήνυμα αφορά έλεγχο ταυτότητας.

1.1.6 Token Requestor ID

Είναι ένα ID το οποίο αποτελείται από ένα μοναδικό αριθμό, ο οποίος χαρακτηρίζει τον TSP και έναν ακόμα αναγνωριστικό το οποίο παράγεται από τον TSP σε κάθε αίτημα.

Θέσεις 1-3: Ο μοναδικός κωδικός του Token Service Provider

Θέσεις 4-11: Αποδίδετε από τον TSP σε κάθε οντότητα που αιτείτε ένα token για ένα συγκεκριμένο πεδίο εφαρμογής.

1.1.7 Token Assurance Level

Είναι η τιμή με το επίπεδο διασφάλισης που παρέχει ο TSP για να δείξει το επίπεδο εμπιστοσύνης του payment token σε σχέση με το PAN και προσδιορίζεται ως αποτέλεσμα του τύπου του ID&V το οποίο πραγματοποιήθηκε και της οντότητας που το εκτέλεσε.

1.1.8 Token Assurance Data

Επίσης ένα προαιρετικό στοιχείο το οποίο περιλαμβάνει επιπλέον πληροφορίες σχετικά με το δεδομένα που συμμετείχαν στην απόδοση του Assurance Level.

1.1.9 Token Cryptogram

Είναι ένα κρυπτογράφημα το οποίο παράγεται μοναδικά κατά την διενέργεια μιας συναλλαγής και αποστέλλεται μαζί με το payment token για την επικύρωση της εξουσιοδοτημένης χρήσης του. Το token cryptogram μπορεί να χαρακτηριστεί και ως dynamic CVV κατά τα πρότυπα του EMV και για τον υπολογισμό του λαμβάνονται υπόψη διάφορα δεδομένα που χαρακτηρίζουν μια συναλλαγή. Το Token Cryptogram είναι κρυπτογραφημένο με μοναδικό κλειδί το οποίο παράγεται μαζί με το payment token.

1.2 Token Service Provider (TSP)

Ένας Token Service Provider αποτελεί μια ανεξάρτητη οντότητα εντός του tokenisation οικοσυστήματος, ο οποίος είναι υπεύθυνος τόσο για την αδιάληπτη έκδοση και παροχή των payment tokens στους αιτούντες όσο και στην παροχή όλων των υπηρεσιών που σχετίζονται με αυτά.

Ορισμένες από τις αρμοδιότητες ενός TSP είναι [3] :

- Η έκδοση των payment tokens
- Η διαχείριση και διατήρηση των payment tokens σε ασφαλές σημείο
- Η εφαρμογή κανόνων ασφάλειας
- Η παροχή payment tokens στους αιτούντες
- Οι υπηρεσίες μητρώου

Το σύστημα των υπηρεσιών που ένας TSP παρέχει αποτελείται από τα παρακάτω δύο βασικά υποσυστήματα:

- Payment Token Provisioning Platform
- Payment Token Transaction Platform

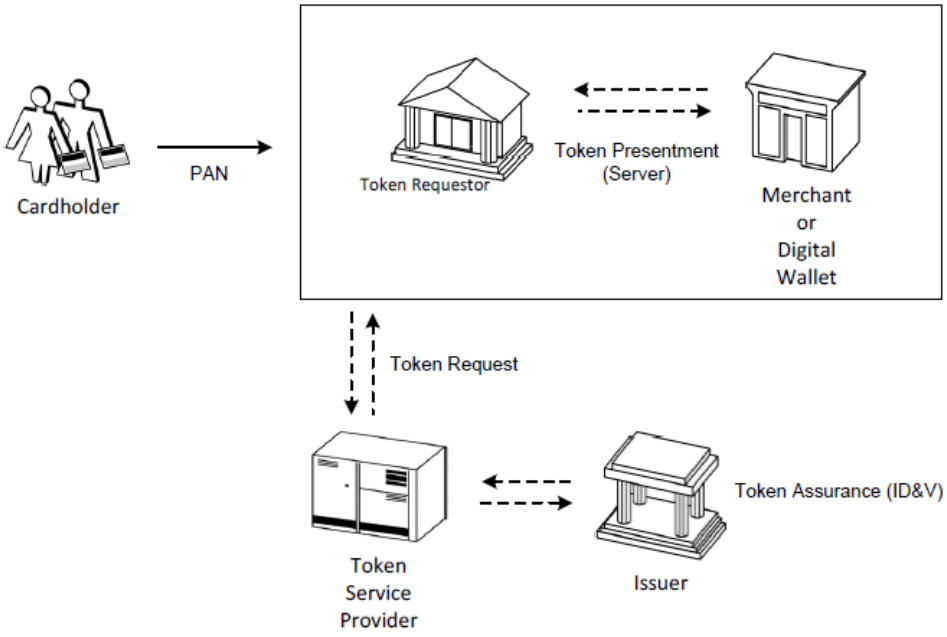
1.2.1 Provision Platform

Για την μετατροπή ενός PAN σε payment token πρέπει ο κάτοχος της κάρτας (Cardholder) μέσω μιας εξουσιοδοτημένης οντότητας (Token Requestor, Merchant) να στείλει σχετικό αίτημα στον TSP, παρέχοντας του ταυτόχρονα τα απαραίτητα διαπιστευτήρια προκειμένου να αποδείξει ότι είναι ο πραγματικός κάτοχος της κάρτας. Όταν ο TSP λάβει κάποιο αίτημα για την δημιουργία ενός payment token, εκτελεί ενέργειες ταυτοποίησης και επαλήθευσης (ID&V) προωθώντας μέρος ή το σύνολο των διαπιστευτηρίων που έχει λάβει στον εκδότη της κάρτας. Ο εκδότης της κάρτας με την σειρά του εκτελεί επίσης αντίστοιχες διεργασίες ID&V σύμφωνα με τις δικές του πολιτικές και επιστρέφει το αποτέλεσμα στον TSP.

Εφόσον τα στοιχεία της ταυτοποίησης και επαλήθευσης είναι επαρκή και έχει λάβει και τη θετική απάντηση από τον εκδότη της κάρτας, τότε ο TSP εκτελεί μια λειτουργία tokenization η οποία αποτελείται από τις παρακάτω ενέργειες :

- Δημιουργία ένας payment token με την ίδια μορφή που είχε και το PAN (BIN, μήκος).
- Καθορισμός των χαρακτηριστικών στοιχείων (elements) του payment token.

- Αποθήκευση του payment token μαζί με το PAN και το PAN Expiry Date σε ασφαλές μέρος.
- Προώθηση του payment token και ορισμένων elements στον αιτούντα.

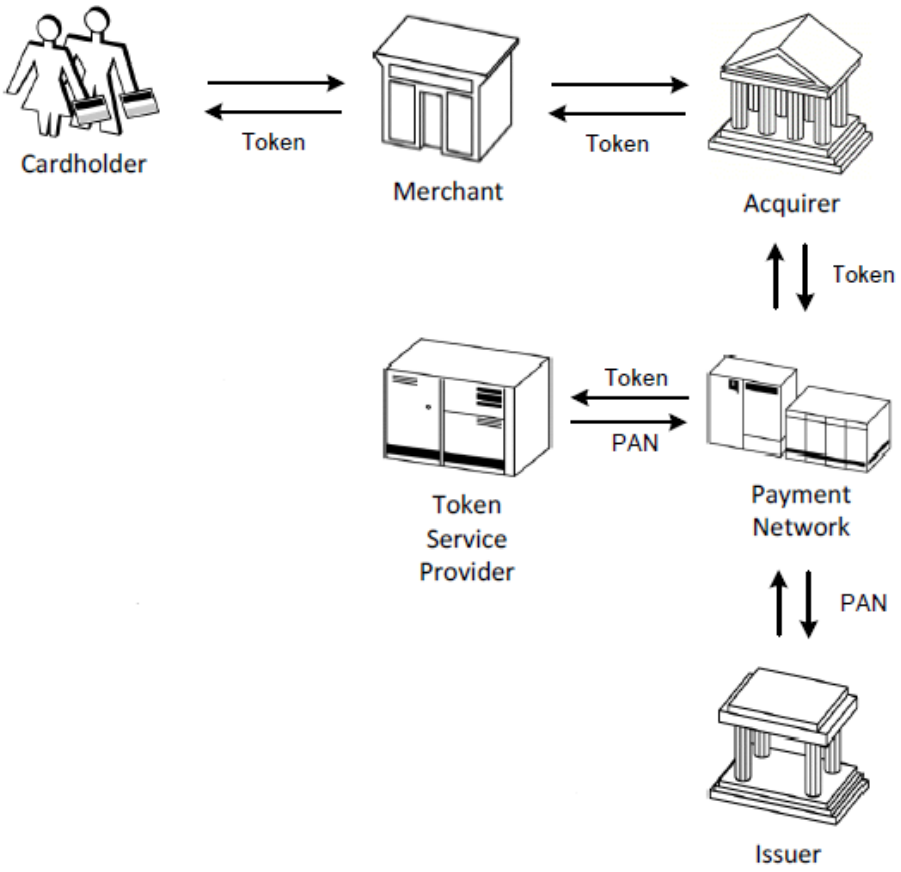


Σχήμα 2: Provision Platform

1.2.2 Transaction Platform

Κατά την διενέργεια μιας ηλεκτρονικής συναλλαγής με payment token, το transaction platform αναλαμβάνει την διαδικασία μετατροπής του payment token στο πραγματικό PAN εκτελώντας μια λειτουργία de-tokenisation η οποία αποτελείται από τις παρακάτω ενέργειες:

- Διενέργεια ελέγχων σχετικά με την εγκυρότητα του payment token (Expiry Date, PoS Entry Mode, Cryptogram κ.α.).
- Εάν το payment token δεν είναι έγκυρο για την συγκεκριμένη συναλλαγή τότε απορρίπτεται αμέσως η συναλλαγή, διαφορετικά ανακτάτε από την βάση το PAN και το PAN Expiry Date και εκτελείται το επόμενο βήμα.
- Προώθηση της συναλλαγής στον εκδότη της κάρτας αντικαθιστώντας το payment token με το πραγματικό PAN και το PAN Expiry Date.



Σχήμα 3: Transaction Platform

2. Radio Frequency Identification

Η τεχνολογία Radio Frequency Identification (RFID) είναι γνωστή εδώ και αρκετές δεκαετίες με την πρώτη σημαντική εφαρμογής της στην διάρκεια του δεύτερου παγκόσμιου πολέμου, όπου τα πολεμικά αεροσκάφη εφοδιάζοντας με αναγνωριστικές ασύρματες συσκευές προκειμένου να μπορούν να αναγνωριστούν από το έδαφος τα φιλικά και τα εχθρικά αεροσκάφη από τους συμμάχους. Οι πρώτες εμπορικές χρήσεις της RFID τεχνολογίας, εμφανίστηκαν την δεκαετία του 60 σε αγαθά μεγάλης αξίας για την αποτροπή κλοπής. Τα επόμενα χρόνια η ανάπτυξη της τεχνολογίας έβρισκε εφαρμογές σε όλο και περισσότερους τομείς και σήμερα πλέον έχουν μπει στην καθημερινότητα όλων μας. Οι εκτιμήσεις μάλιστα των οργανισμών μιλάνε για ραγδαία αύξηση της χρήσης τους τα επόμενα χρόνια σε υφιστάμενες ή και νέες εφαρμογές όπως είναι για παράδειγμα η τεχνολογία NFC στις έξυπνες συσκευές η οποία έχει ήδη υιοθετεί από πολλές εταιρίες και η χρήση της αναμένεται να αυξηθεί σημαντικά σε πολύ σύντομο χρονικό διάστημα.

Ο όρος RFID χρησιμοποιείται για να περιγράψει τα συστήματα όπου ένας σταθμός βάσης ή κάποιος αναγνώστης είναι ικανός να αναγνωρίσει μια ηλεκτρονική συσκευή η αλλιώς ετικέτα χρησιμοποιώντας έναν ασύρματο μηχανισμό μετάδοσης με την χρήση ηλεκτρομαγνητικών συχνοτήτων

2.1 Αναγνώστες

Οι RFID αναγνώστες χρησιμοποιούνται για να αναγνωρίζουν τις RFID ετικέτες και να μεταδίδουν RF ενέργεια μέσω μίας ή περισσότερων κεραιών. Η ετικέτα λαμβάνοντας αυτήν την ενέργεια μέσω της επαγωγικής ιδιότητας την μετατρέπει σε ηλεκτρική. Στην συνέχεια αυτή η ενέργεια είναι ικανή να τροφοδοτήσει το κύκλωμα της ετικέτας η οποία περιέχει την ταυτότητα της και η οποία λαμβάνεται από την RFID κεραία. Αυτός ο τρόπος λειτουργίας και επικοινωνίας του RFID αναγνώστη και της RFID ετικέτας, αποτελεί το πιο απλό σενάριο αυτού του είδους επικοινωνίας αλλά δεν είναι και ο μοναδικός.

Οι αναγνώστες υπάρχουν σε διαφορά σχήματα και μεγέθη, και μπορεί να είναι είτε σταθεροί, είτε φορητοί.

Κάποια βασικά χαρακτηριστικά τους είναι:

***Πρόγραμμα διασύνδεσης**:* Το πρόγραμμα διασύνδεσης εφαρμογής του αναγνώστη αποτελεί το περιβάλλον επικοινωνίας για την ανάγνωση των RFID ετικετών. Επίσης περιέχει λειτουργίες για την παραμετροποίηση, καταγραφή και γενικότερα τον έλεγχο του αναγνώστη.

***Επικοινωνία**:* Οι αναγνώστες είναι συσκευές διασύνδεσης σε ένα υποσύνολο δικτύου.

***Διαχείριση γεγονότων**:* Όταν ένας αναγνώστης διαβάσει μια ετικέτα τότε η διαδικασία αυτή ονομάζεται παρατήρηση. Η διαχείριση γεγονότων αφορά την διαχείριση των παρατηρήσεων εντός του δίκτύου.

***Κεραία**:* Το σύστημα κεραίας στον αναγνώστη αφορά μια ή περισσότερες κεραίες που η βασική τους λειτουργία είναι η ανάγνωση των RFID ετικετών.

Οι αναγνώστες ανεξάρτητα από το πρωτόκολλο επικοινωνίας με τον host, πρέπει να μπορούν να ανταπεξέλθουν σε τρείς βασικούς τύπους επικοινωνίας:

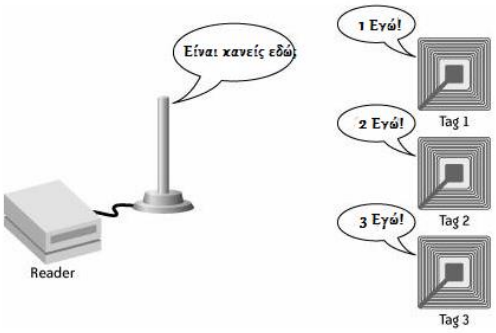
- Τις εντολές που περνούν από τον host στον αναγνώστη
- Τις επισημάνσεις που περνούν από τον αναγνώστη στον host
- Τις ειδοποιήσεις από τον αναγνώστη στον host

Σχήμα 4: Επικοινωνία host – αναγνώστη

2.2 Ετικέτες

Ο αναγνώστης μπορεί να αναγνωρίσει ένα αντικείμενο διαβάζοντας την RFID ετικέτα που είναι προσαρμοσμένη πάνω σε αυτή. Το περίβλημα των ετικετών μπορεί να είναι κάποιο πλαστικό αντικείμενο, μια γυάλινη κάψουλα, μια χάρτινη ετικέτα, ή κάποιο μεταλλικό περίβλημα. Τέλος μπορεί να είναι κολλημένες σε ένα πακέτο, ενσωματωμένες σε έναν άνθρωπο ή ζώο, πάνω σε κάποιο ρούχο κ.α.

Για να γίνει κατανοητό πώς μια RFID ετικέτα ειδοποιεί έναν αναγνώστη για την ταυτότητα και την παρουσία της, ακολουθεί το παρακάτω σενάριο που περιγράφεται στην *σχήμα 5*. Σε αυτήν την εικόνα ο RFID αναγνώστης μεταδίδει σήματα με μια σταθερή συχνότητα. Οι ετικέτες λαμβάνοντας τα σήματα αυτά παίρνουν την απαραίτητη ενέργεια ώστε να ανακλάσουν το σήμα πίσω στον αναγνώστη. Οι ετικέτες διαμορφώνουν το σήμα για να στείλουν κάποια πληροφορία όπως για παράδειγμα ένα ID αριθμό.



Σχήμα 5: Επικοινωνία μεταξύ RFID αναγνώστη και RFID ετικετών

Μερικά βασικά χαρακτηριστικά των RFID ετικετών περιλαμβάνουν:

***Συσκευασία**:* Η συσκευασία αναφέρεται στο περίβλημα των RFID ετικετών.

***Σύνδεση**:* Αναφέρεται στον τρόπο με τον οποίο ο αναγνώστης και η ετικέτα επικοινωνούν.

***Ενέργεια**:* Αναφέρεται στον τρόπο με τον οποίο τροφοδοτούνται οι RFID ετικέτες. Τις διακρίνουμε σε παθητικές, ενεργές και “διπλού δρόμου”.

***Πληροφορία**:* Αναφέρεται στην πληροφορία που μπορεί να αποθηκευτεί στις RFID ετικέτες.

2.2.1 Χωρητικότητα και υπολογιστική ικανότητα

Οι RFID ετικέτες χωρίζονται επίσης σε κατηγορίες ανάλογα με την ικανότητα που έχουν να αποθηκεύουν πληροφορία. Οι πιο απλές ετικέτες έχουν ικανότητα αποθήκευσης ενός μόνο bit. Τα συστήματα που βασίζονται σε αυτές τις ετικέτες χρησιμοποιούνται συνήθως σε βιβλιοθήκες και καταστήματα ενδυμασίας για προστασία από κλοπή και την αναγνώριση παρουσίας ή απουσίας ενός αντικειμένου. Κάποιες ετικέτες έχουν την ικανότητα αποθήκευσης δεδομένων μερικών KBytes. Οι ετικέτες με μεγαλύτερη χωρητικότητα είναι συνήθως ενεργές και το κόστος τους ανεβαίνει σημαντικά.

2.2.2 Πηγή ενέργειας

Ένας συνήθης τρόπος για την κατηγοριοποίηση των ετικετών είναι η πηγή ενέργειάς τους. Αυτός επίσης είναι ένας παράγοντας για να προσδιοριστεί το κόστος και ο χρόνος ζωής τους. Οι παθητικές ετικέτες παίρνουν όλη την ενέργεια τους από τον αναγνώστη. Οι ενεργητικές χρησιμοποιούν μια μπαταρία για να τροφοδοτήσουν την επικοινωνία τους με τον αναγνώστη, τον επεξεργαστή, την μνήμη και ίσως κάποιους αισθητήρες. Κάποιες ετικέτες οι οποίες χρησιμοποιούν μπαταρία για ορισμένες λειτουργίες τους αλλά χρησιμοποιούν την ενέργεια του αναγνώστη για την επικοινωνία είναι επίσης παθητικές, ωστόσο αναφέρονται και ως ημι-παθητικές. Τέλος ο τύπος ετικέτας που χρησιμοποιεί μπαταρία για την λειτουργία του αλλά μπορεί να επικοινωνήσει με άλλες ετικέτες χωρίς την ανάγκη κάποιου αναγνώστη ονομάζονται ετικέτες διπλού δρόμου.

Είναι προφανές ότι η ενσωμάτωση μπαταρίας στις ενεργές ετικέτες αυξάνει το κόστος τους. Το πλεονέκτημα βέβαια σε σχέση με τις παθητικές ετικέτες, είναι η μεγάλη απόσταση επικοινωνίας με τον αναγνώστη.

2.3 Συχνότητα λειτουργίας

Η συχνότητα λειτουργίας είναι η ηλεκτρομαγνητική συχνότητα που χρησιμοποιείται από την ετικέτα για να επικοινωνήσει και να λάβει ενέργεια. Το ηλεκτρομαγνητικό φάσμα λειτουργίας των RFIDs διακρίνεται σε χαμηλές συχνότητες (LF), υψηλές (HF), πολύ υψηλές (UHF) και μικροκυματικές.

Συχνότητα	Περιοχή συχνοτήτων	ISM Συχνότητες	Απόσταση λειτουργίας	Εφαρμογές
LF	30300 kHz	< 135 kHz	50 εκατοστά	Αναγνώριση κατοικίδιων και αντικειμένων με υψηλή περιεκτικότητα σε νερό
HF	330 MHz	6.78 MHz 13.56 MHz 27.125 MHz 40.680 MHz	3 μέτρα	Συστήματα ελέγχου προσπέλασης, NFC
UHF	300 MHz-3 GHz	6.78 MHz 13.56 MHz 27.125 MHz 40.680 MHz	9 μέτρα	Κουτιά και παλέτες
Microwave	> 3 GHz	2.45 GHz 5.8 GHz 24.125 GHz	> 10 μέτρα	Αναγνώριση οχημάτων

Πίνακας 1: Συχνότητες RFID

3. Near Field Communication

Η τεχνολογία Near Field Communication (NFC) αφορά την ασύρματη μετάδοση δεδομένων μεταξύ δυο συσκευών σε μέγιστες αποστάσεις των 10 εκατοστών αν και συνήθως είναι μικρότερες των 5 εκατοστών. Επιτρέπει την γρήγορη ανάγνωση και εγγραφή δεδομένων και εκλαμβάνεται ως απόδειξη φυσικής παρουσίας. Αξιοποιείται μέσω κινητών συσκευών όπως είναι τα smartphones και τα tablets και χρησιμοποιούνται σε διάφορες εφαρμογές με κυριότερες τις ηλεκτρονικές πληρωμές και τον έλεγχο πρόσβασης.

Το πρωτόκολλο επικοινωνίας λειτουργεί στη συχνότητα 13.56MHz η οποία είναι μέρος του RFID, πληροί τις προδιαγραφές των στάνταρτ ISO/IEC 14443 A & B, και Felica (ISO 18092) και μεταφέρει δεδομένα με ρυθμό έως και 424 kbps.

Οι τρόποι λειτουργίας που υποστηρίζονται είναι οι ακόλουθοι τρεις:

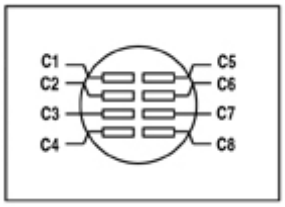
- Λειτουργία γρήγορης ανάγνωσης/εγγραφής (read/write mode, 48 Bytes-9KB)
- Λειτουργία Peer-to-Peer μέσω σύνδεσης δύο συσκευών ομότιμης σχέσης
- Λειτουργία NFC εξομοίωσης καρτών που επιτρέπει σε μια συσκευή να συμπεριφέρεται στα πρότυπα μιας έξυπνης κάρτας.

Η τεχνολογία αναπτύσσεται και προωθείται κυρίως από το NFC Forum, το οποίο ιδρύθηκε το 2004 και σήμερα αριθμεί περισσότερα από 260 μέλη από τον χώρο των κατασκευαστών ηλεκτρονικών συσκευών, των οργανισμών πληρωμών και των προγραμματιστών εφαρμογών.

Αρκετές εταιρίες έχουν υιοθετήσει την υποστήριξη αυτής της τεχνολογίες όπως είναι η Nokia, η Google, η Samsung, η RIM κ.α. Κάποιες από αυτές έχουν ήδη κυκλοφορήσει έξυπνες κινητές συσκευές με ενσωματωμένη την υποστήριξη του NFC, ενώ αρκετές ακόμα εταιρίες της αγοράς έχουν ανακοινώσει ότι θα κυκλοφορήσουν σύντομα προϊόντα με ενσωματωμένη NFC τεχνολογία.

4. Secure Element

Το Secure Element (SE) είναι ένα ανθεκτικό στην παραβίαση chip, συμβατό με το ISO 7816 standard, το οποίο συνήθως ενσωματώνεται στο NFC chip των έξυπνων συσκευών και χρησιμοποιείται για να αποθηκεύονται και να φυλάσσονται προστατευμένα ευαίσθητα δεδομένα. Τα συγκεκριμένα chip εκτός από μνήμη διαθέτουν και μικροεπεξεργαστή με τον οποίο εκτελούν κρυπτογραφικές πράξεις. Εκτός από την προστασία των δεδομένων με την χρήση κρυπτογραφικών αλγορίθμων για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων το SE χρησιμοποιείται επιπλέον για αποθήκευση και διαχείριση κλειδιών.



Σχήμα 6: Smart Card Layout

Όπως φαίνεται στο παραπάνω σχήμα το chip διαθέτει οκτώ επαφές, από τις οποίες όμως μόνο οι πέντε είναι λειτουργικές:

C1: Supply Voltage (VCC)
C2: Reset (RST)
C3: Clock (CLK)
C4: RFU
C5: Ground (GND)
C6: Programming Voltage (Vpp)
C7: Input/Output (I/O)
C8: RFU

Οι επαφές C4 και C8 δεν χρησιμοποιούνται αλλά σύμφωνα με το πρότυπο ISO πρέπει να υφίστανται στο κύκλωμα και είναι δεσμευμένες για μελλοντική χρήση.

5. EMVCo

Το EMVCo κατέχει ένα ιδιωτικό πρωτόκολλο το οποίο σχεδιάστηκε και αναπτύχθηκε από τους οργανισμούς τραπεζικών καρτών Europay, Mastercard και Visa, οι οποίοι από κοινού έγραψαν τους κανόνες και τις προδιαγραφές που θα διέπουν την χρήση των έξυπνων καρτών μέσω των συσκευών (EFT-POS, ATM) εκτέλεσης οικονομικών συναλλαγών.

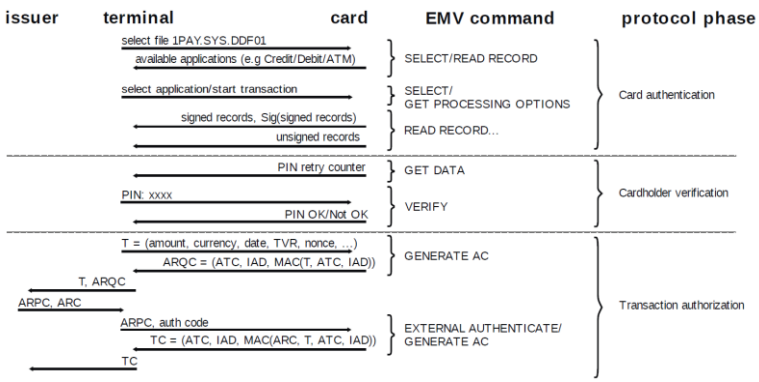
Οι στόχοι του EMV ήταν η μείωση της αυξανομένης απάτης, η αποτελεσματικότερη διαχείριση του παγκοσμίως αυξανόμενου όγκου συναλλαγών και η διασφάλιση της σωστής συνεργασίας μεταξύ διαφορετικών εφαρμογών χρήσης χρεωστικών/πιστωτικών καρτών.

Αν και έχει επιτευχθεί σημαντική μείωση της απάτης όπου έχει υλοποιηθεί και εφαρμοστεί το EMV, ωστόσο το ίδιο το EMV δεν έχει καταφέρει να μειώσει το λεγόμενο cross platform fraud, δεδομένου ότι δεν εμποδίσει την ανάγνωση των στοιχείων της κάρτας από τρίτους, τα οποία στην συνέχεια μπορούν να χρησιμοποιηθούν σε άλλα λιγότερο ασφαλή κανάλια όπως είναι για παράδειγμα το eCommerce στο οποίο δεν απαιτείται η φυσική παρουσία της κάρτας.

5.1 Επίπεδα Ασφάλειας

Κατά την διάρκεια μιας EMV συναλλαγής πραγματοποιούνται τα παρακάτω τρία επίπεδα ασφάλειας:

1) Card Authentication
2) Cardholder Verification
3) Transaction Authorization



Σχήμα 7: Οι τρεις φάσεις ασφάλειας του EMV πρωτοκόλλου

5.1.1 Card Authentication

Επειδή μια EMV κάρτα ενδέχεται να έχει παραπάνω από μια διαθέσιμες εφαρμογές, η πρώτη ενέργεια κατά την εισαγωγή της σε έναν «έξυπνο αναγνώστη» είναι μια αίτηση από το τερματικό για την αποστολή από την κάρτα των διαθέσιμων εφαρμογών . Αφού η κάρτα αποστείλει τα διαθέσιμα applications γίνεται έλεγχος από το τερματικό αν υποστηρίζει και αυτό κάποια από τις εφαρμογές της κάρτας . Αν τελικά βρεθούν ένα ή περισσότερα κοινά applications ακολουθεί η διαδικασία επιλογής του επιθυμητού (πχ. Visa Credit) μέσω της εντολής “Get Processing options”. Αμέσως μετά με την εντολή “Read Record” και τις ανάλογες παραμέτρους, το τερματικό διαβάζει από την κάρτα διάφορες πληροφορίες που αφορούν είτε τον κάτοχο, είτε οδηγίες για την τρόπο εκτέλεση της συναλλαγής, καθώς επίσης και τις ψηφιακές υπογραφές και τα ψηφιακά πιστοποιητικά της κάρτας.

Έχοντας πλέον όλες τις παραπάνω πληροφορίες το τερματικό μπορεί να επιβεβαιώσει ότι η κάρτα είναι γνήσια και πως τα περιεχόμενα της δεν έχουν τροποποιηθεί.

Ανάλογα με τον τύπο της «έξυπνης κάρτας» υπάρχουν οι παρακάτω τρεις τρόποι πιστοποίησης:

1) Static Data Authentication (SDA)
2) Dynamic Data Authentication (DDA)
3) Combined Data Authentication (CDA)

5.1.2 Cardholder Verification

Η επιλογή του τρόπου επαλήθευσης του κατόχου της κάρτας γίνεται με μια διαδικασία διαπραγμάτευσης μεταξύ του τερματικού και της κάρτας. Η κάρτα έχει μια λίστα με τους επιτρεπτούς τρόπους επαλήθευσης (**C**ard **V**erification **L**ist) και το τερματικό αντίστοιχα υποστηρίζει κάποιες από τις διαθέσιμες μεθόδους που υποστηρίζονται από το EMV.

Την πρώτη μέθοδο που θα βρει το τερματικό στην CMV λίστα της κάρτας την οποία υποστηρίζει και αυτό, θα την επιλέξει ως μέθοδο ταυτοποίησης που θα χρησιμοποιηθεί για την συγκεκριμένη συναλλαγή.

Οι διαθέσιμοι τρόποι ταυτοποίησης του κατόχου της κάρτας είναι οι παρακάτω:

1) Υπογραφή
2) Offline plaintext PIN

3) Offline enciphered PIN (RSA)
4) Online PIN (DES/3DES)

Εκτός από την υπογραφή και του Offline plaintext PIN, για τις υπόλοιπες μεθόδους απαιτείται η χρήση κρυπτογραφικών αλγόριθμων.

5.1.3 Transaction Authorization

Στο τρίτο και τελευταίο βήμα το τερματικό ζητάει από την κάρτα ένα **M**essage **A**uthentication **C**ode με τα στοιχεία της συναλλαγής για να το αποστείλει στην εκδότρια τράπεζα. Όταν η τράπεζα λάβει το αίτημα για έγκριση της συναλλαγής θα κάνει διαφόρους ελέγχους όπως αποφυγής απάτης, ανάλυσης ρίσκου, αν η κάρτα είναι ενεργή και αν το ζητούμενο ποσό είναι εντός του πιστωτικού ορίου κλπ. και αφού ολοκληρωθούν όλοι οι έλεγχοι θα επιστρέψει το ARC (**A**uthorization **R**esponse **C**ode) και το ARPC (**A**uthorization **R**es**P**onse **C**ryptogram).

Η διαδικασία αυτή περιγράφεται αναλυτικά με τα παρακάτω βήματα:

- Το τερματικό κάνει μια ARQC (**A**uthorization **R**e**Q**uest **C**ryptogram) αίτηση στην κάρτα
- Η κάρτα υπολογίζει το MAC λαμβάνοντας υπόψη τις σημαντικές πληροφορίες τις συναλλαγής και το στέλνει στο τερματικό
- Το τερματικό στέλνει τα στοιχεία της συναλλαγής μαζί με το MAC value στην εκδότρια τράπεζα (μέσω του συστημάτων συναλλαγών)
- Η τράπεζα κάνει διάφορους ελέγχους καθώς και την επαλήθευση του MAC (Η επαλήθευση του MAC πιστοποιεί ότι η κάρτα που χρησιμοποιήθηκε ήταν έγκυρη) και απαντάει με έναν κωδικό έγκρισης ARC (**A**uthorization **R**esponse **C**ode) και ένα ARPC (**A**uthorization **R**es**P**onse **C**ode) για να πιστοποιήσει και στην κάρτα ότι το σύστημα που έδωσε την έγκριση ήταν έγκυρο. Το ARPC είναι ένα MAC του ARQC xor ARC:

  - $ARPC = 3DES_K(ARQC \oplus ARC)$

- Η κάρτα επαληθεύει το ARPC και ενημερώνει το τερματικό
- Εάν το ARPC ήταν έγκυρο, τότε το τερματικό ζητάει από την κάρτα ένα πιστοποιητικό συναλλαγής (**T**ransaction **C**ertificate)

- Η κάρτα υπολογίζει το TC και το στέλνει στο τερματικό
- Τέλος το τερματικό προωθεί το TC στην εκδότρια τράπεζα

Με την μέθοδο αυτή γίνεται πιστοποίηση τόσο από την τράπεζα ότι η κάρτα ήταν έγκυρη αλλά και η κάρτα πιστοποιεί ότι η τράπεζα η οποία έδωσε την έγκριση ήταν είναι και αυτή έγκυρη.

5.2 Contactless

Το EMVCo έχει επίσης προσαρμόσει τις προδιαγραφές του πρωτοκόλλου του, το οποίο αρχικά ανέπτυξε για την εφαρμογή του στην contact κάρτες, έτσι ώστε να είναι συμβατό και για της contactless κάρτες αλλά παράλληλα να εφαρμόζει τα ίδια επίπεδα ασφάλειας. Οι προδιαγραφές αυτές περιγράφονται σε δέκα ξεχωριστά βιβλία σε σχέση με τα τέσσερα των contact καρτών.

6. Apple Pay

Σύμφωνα με τις δηλώσεις που έγιναν κατά την παρουσίαση της υπηρεσίας Apple Pay, η Apple δημιούργησε μια εντελώς νέα μέθοδο πληρωμών, τα βασικά χαρακτηριστικά της οποίας είναι η ευκολία χρήσης, η ασφάλεια και η προστασία της ιδιωτικότητας. Παρόλο που ακολούθησε μια εκτενής παρουσίαση του τρόπου χρήσης, δεν έγινε αντίστοιχη ανάλυση του τρόπου λειτουργίας της υπηρεσίας και των τεχνολογιών ή των τεχνικών που εφαρμόζονται για την υλοποίηση της. Το Apple Pay είναι πράγματι μια νέα μέθοδος πληρωμών, η οποία όμως βασίζεται σε υπάρχουσες τεχνολογίες και τεχνολογικές μεθόδους όπως είναι το NFC, το Secure Element (SE) στο οποίο αποθηκεύονται τα στοιχεία της κάρτας, το Passbook για την διαχείριση των καρτών, το Touch ID κ.α.

Το εντελώς νέο χαρακτηριστικό είναι ότι με το Apple Pay αντικαθίσταται η φυσική κάρτα από την ίδια την συσκευή. Η ιδέα αυτή βέβαια δεν είναι νέα και υπάρχουν ήδη και άλλες υλοποιήσεις όπου μια κινητή συσκευή μπορεί να χρησιμοποιηθεί ως παρουσία κάρτας, αυτή είναι άλλωστε και η βασική ιδέα που υλοποιείται με το NFC. Η διαφορά είναι ότι στις υπάρχουσες υλοποιήσεις απαιτείται η προμήθεια ειδικού Subscriber Identity Module (SIM), το οποίο ενσωματώνει το SE και προϋποθέτει την συνεργασία της εκδότριας τράπεζας με τον Mobile Network Operator (MNO). Στο συγκεκριμένο μοντέλο ο MNO κατέχει δεσπόζουσα θέση μιας και είναι ο κάτοχος του SE, γεγονός που τον καθιστά βασικό εταίρο σχετικά με το μοίρασμα των μεριδίων των εμπλεκόμενων μερών. Αντίθετα στο Apple Pay δεν απαιτείται ειδική SIM κάρτα μιας και το SE ενσωματώνεται στις συσκευές της εταιρίας και ο χρήστης μπορεί να εισάγει στη συσκευή του, οποιαδήποτε κάρτα με την μοναδική προϋπόθεση η εκδότρια τράπεζα να είναι συμβεβλημένη με την υπηρεσία. Πως όμως επιτυγχάνεται η εισαγωγή μιας κάρτας στην κινητή συσκευή με ασφαλή τρόπο και χωρίς τον κίνδυνο κάποιος τρίτος να χρησιμοποιήσει την συσκευή για να πραγματοποιήσει αγορές; Για την επίτευξη των παραπάνω στόχων η Apple υιοθέτησε την τεχνική του tokenisation και συνδύασε υπάρχουσες τεχνολογίες (Touch ID, Passcode, Skin Sensor, Find My iPhone) που διαθέτουν οι συσκευές της, για τον έλεγχο εξουσιοδοτημένης πρόσβασης.

6.1 Passbook

Το Passbook είναι μια εφαρμογή της Apple η οποία ενσωματώθηκε στο iOS 6 σε όλες τις συσκευές της εταιρίας και αρχικά παρουσιάστηκε ως ένας εύκολος τρόπος αποθήκευσης

και διαχείρισης εισιτήριων, κουπονιών, καρτών επιβίβασης, καρτών καταστημάτων και πάσης φύσεων καρτών εισόδου [10]. Η εφαρμογή διαθέτει αναγνώριση τόπου και χρόνου και σε συνδυασμό με τα αντίστοιχα χαρακτηριστικά που διαθέτουν οι κάρτες που εισάγονται σε αυτή, παρέχεται η σχετική ενημέρωση στους χρήστες όταν κάποιο από τα παραπάνω κριτήρια ικανοποιείται. Για παράδειγμα εμφανίζεται στην οθόνη του χρήστη η κάρτα επιβίβασης μερικές ώρες πριν από την πτήση ή εμφανίζεται η κάρτα ενός καταστήματος όταν ο χρήστης κινείται σε κοντινό με αυτό σημείο.

Με την εισαγωγή της υπηρεσίας Apple Pay, το passbook γίνεται η βασική εφαρμογή διαχείρισης των τραπεζικών καρτών. Μέσω αυτής της εφαρμογής γίνεται η εγγραφή μιας κάρτας στην υπηρεσία και μέσω αυτής γίνεται η επιλογή της κάρτας που θα χρησιμοποιηθεί κατά την διάρκεια μιας πληρωμής.

6.2 Touch ID

Με την ανάπτυξη χιλιάδων εφαρμογών στις έξυπνες συσκευές πολλές από τις οποίες αποκτούν πρόσβαση σε προσωπικά δεδομένα του χρήστη κατέστη αναγκαία η υλοποίηση ελέγχου πρόσβασης όπου ο χρήστης ταυτοποιείται, προκειμένου να αποκτήσει πρόσβαση σε αυτό. Η ταυτοποίηση μπορεί να γίνει είτε με κάποιο αναγνωριστικό κωδικό που ο χρήστης πρέπει να θυμάται ή με βιομετρικά στοιχεία όπως το δακτυλικό του αποτύπωμα στην περίπτωση του Touch ID.

Το Touch ID αποτελείται από έναν αισθητήρα ανάγνωσης και αναγνώρισης του δαχτυλικού αποτυπώματος και για την ταυτοποίηση του χρήστη με την χρήση του Touch ID απαιτείται πρώτα να γίνει εγγραφή ενός ή περισσότερων δακτυλικών αποτυπωμάτων.

Κάθε δακτυλικό αποτύπωμα είναι μοναδικό, έτσι είναι σπάνιο ακόμη και ένα μικρό τμήμα από δύο ξεχωριστά δακτυλικά αποτυπώματα είναι αρκετά όμοια. Η πιθανότητα να συμβεί αυτό είναι 1 στις 50.000 και φυσικά είναι πολύ καλύτερο από τη 1 στις 10.000 πιθανότητες να μαντέψουν ένα 4-ψήφιο κωδικό πρόσβασης. Αντ' αυτού, η μια στις 50.000 πιθανότητες σημαίνει ότι απαιτείτε προσπάθεια με μέχρι 50.000 διαφορετικά δακτυλικά αποτυπώματα μέχρι δυνητικά να βρεθεί μια τυχαία αντιστοιχία. Το Touch ID όμως επιτρέπει μόνο πέντε συνεχόμενες ανεπιτυχείς προσπάθειες ανάγνωσης δακτυλικού αποτυπώματος και μετά απαιτείται η εισαγωγή του κωδικού πρόσβασης [11].

Το Touch ID δεν αποθηκεύει εικόνες των δακτυλικών αποτυπωμάτων αλλά μόνο μια μαθηματική αναπαράσταση τους. Από την μαθηματική αναπαράσταση δεν είναι δυνατόν

να αναπαράγει κάποιος την πραγματική εικόνα του δακτυλικού αποτυπώματος. Το τσιπ στη συσκευή έχει σχεδιαστεί με μια σύνθετη αρχιτεκτονική ασφάλειας που ονομάζεται Secure Enclave και έχει αναπτυχθεί αποκλειστικά για την προστασία των δεδομένων του κωδικού πρόσβασης και των δακτυλικών αποτυπωμάτων. Τα δεδομένα των δακτυλικών αποτυπωμάτων, κρυπτογραφούνται και προστατεύονται με ένα κλειδί το οποίο είναι διαθέσιμο μόνο εντός του Secure Enclave. Τα δεδομένα των δακτυλικών αποτυπωμάτων μεταφέρονται εντός του Secure Enclave chip για να ταυτοποιηθούν ότι ταιριάζουν με τα εγγεγραμμένα δακτυλικά αποτυπώματα. Το Secure Enclave είναι τοποθετημένο μακριά από το υπόλοιπα τσιπ και απομονωμένο από το υπόλοιπο iOS. Ως εκ τούτου, τόσο το iOS όσο και οι άλλες εφαρμογές δεν έχουν πρόσβαση στα δεδομένα των δακτυλικών αποτυπωμάτων. Επίσης δεν αποθηκεύεται σε διακομιστές της Apple, ούτε σε αντίγραφα ασφαλείας στο iCloud ή οπουδήποτε αλλού. Πρόσβαση σε αυτό έχει μόνο το Touch ID και δεν μπορεί να χρησιμοποιηθεί για να ταιριάξει με άλλες βάσεις δεδομένων δακτυλικών αποτυπωμάτων [11].

Με την χρήση του Touch ID ο χρήστης μπορεί να αγοράσει περιεχόμενο από το iTunes Store, App Store, και το iBook Store αντί να εισάγει το Apple ID. Η σάρωση του δακτυλικού αποτυπώματος είναι απαραίτητη σε κάθε αγορά. Εάν η συσκευή χαθεί ή κλαπεί, μπορεί αμέσως να απενεργοποιηθεί με την χρήση του Find My iPhone και την επιλογή της κατάστασης απώλειας.

Στην υπηρεσία του Apple Pay, το Touch ID χρησιμοποιείται για την επιβεβαίωση και την ολοκλήρωση μιας συναλλαγής όπως γίνεται με την χρήση του PIN στο κλασσικό τρόπο χρήσης μιας κάρτας.

6.3 Skin Sensor

Για την ασφάλεια χρήσης του Apple Watch η συσκευή διαθέτει έναν αισθητήρα δέρματος. Όταν το ρολόι έρχεται σε επαφή με το δέρμα θα πρέπει να πληκτρολογηθεί ο κωδικός χρήσης που ορίστηκε κατά την εγκατάσταση της συσκευής και έτσι η συσκευή ξεκλειδώνει και παραμένει ξεκλείδωτη για όσο διάστημα βρίσκεται σε επαφή με το δέρμα. Αν για κάποιο λόγο χάσει το ρολόι την επαφή με το δέρμα τότε κλειδώνει αυτόματα και απαιτείται εκ νέου εισαγωγή του κωδικού πρόσβασης όταν έρθει ξανά σε επαφή. Με αυτό τον τρόπο η συσκευή είναι σε θέση να γνωρίζει πότε είναι φορεμένη από εξουσιοδοτημένο χρήστη και πότε όχι.

6.4 Find My iPhone

Η Apple έχει εξοπλίσει όλες τις συσκευές της με την συγκεκριμένη υπηρεσίας, η οποία παρέχει την δυνατότητα στους κατόχους συσκευών που έχουν ενεργοποιημένη αυτή την λειτουργία να έχουν τον έλεγχο των συσκευών τους, είτε μέσω μιας mobile εφαρμογής, είτε μέσω της διαδικτυακής πλατφόρμας iCloud [15]. Αποκτώντας κάποιος πρόσβαση στη συγκεκριμένη υπηρεσία έχει τις παρακάτω επιλογές:

- Εντοπισμός συσκευής
- Αναπαραγωγή ήχου
- Κατάσταση απώλειας
- Σβήσιμο συσκευής

6.4.1 Εντοπισμός συσκευής

Η συγκεκριμένη επιλογή εμφανίζει όλες τις συσκευές που έχουν εγγραφεί με το Apple ID που δόθηκε για την πρόσβαση στην υπηρεσία και εμφανίζει την κατάσταση τους (online, offline). Αν μια συσκευή είναι online εμφανίζεται στον χάρτη με το τρέχον γεωγραφικό στίγμα της, ενώ αν είναι offline εμφανίζεται η τελευταία θέση που εντοπίστηκε η συσκευή όσο παρέμενε online.

6.4.2 Αναπαραγωγή ήχου

Με την επιλογή αυτή, εφόσον η συσκευή είναι online, θα ηχήσει ένας μουσικός τόνος ακόμα και αν είναι σε κατάσταση σίγασης και χρησιμοποιείται όταν κάποια συσκευή εμφανίζεται σε πολύ κοντινό σημείο και δεν μπορεί να εντοπιστεί.

6.4.3 Λειτουργία απώλειας

Με την επιλογή αυτή ζητείται από τον χρήστη της υπηρεσίας η εισαγωγή ενός τηλεφωνικού αριθμού για να επικοινωνήσει μαζί του, αυτός που πιθανών έχει βρει την συσκευή. Με την ολοκλήρωση της εισαγωγής η συσκευή κλειδώνει, ένας μουσικό ήχος αναπαράγεται και ο αριθμός επικοινωνίας εμφανίζεται στην οθόνη της συσκευής.

6.4.4 Σβήσιμο Συσκευής

Εφόσον η συσκευή είναι online θα διαγραφούν άμεσα όλα τα δεδομένα της και θα τεθεί σε εργοστασιακή κατάσταση. Αν η συσκευή είναι offline, η διαδικασία διαγραφής θα εκκινήσει αμέσως μόλις τεθεί σε online κατάσταση.

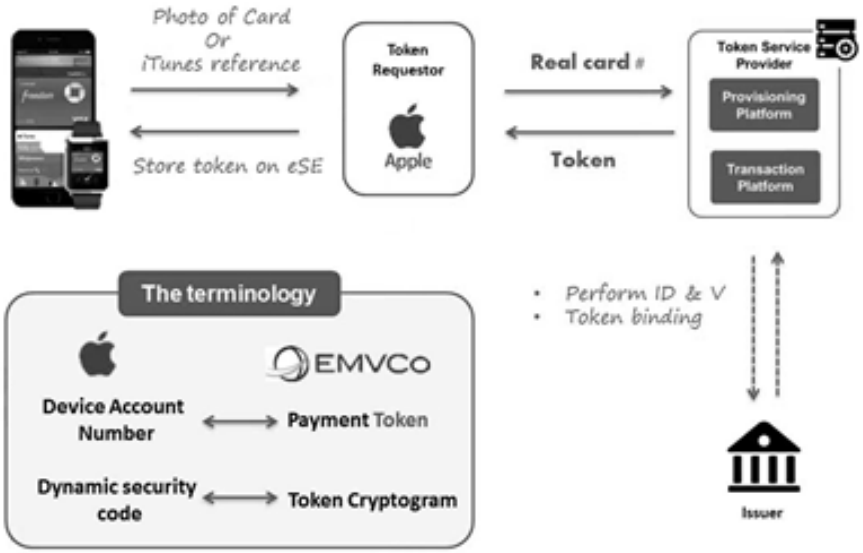
6.5 Τρόπος λειτουργίας

Για την χρήση του συγκεκριμένου τρόπου πληρωμής, ο κάτοχος μιας από τις συσκευές που υποστηρίζουν αυτή την τεχνολογία θα πρέπει πρώτα να καταχωρήσει μια κάρτα η οποία θα πρέπει να έχει εκδοθεί από τράπεζα που συμμετέχει στην υπηρεσία.

6.5.1 Προσθήκη κάρτας

Η εγγραφή μιας κάρτας στην υπηρεσία γίνεται μέσω της εφαρμογής passbook και μπορεί να δηλωθεί είτε μια κάρτα που έχει ήδη καταχωρηθεί στο iTunes, είτε μια νέα η οποία θα προστεθεί με την χρήση της κάμερας. Εφόσον απαιτείται νέα εισαγωγή, ενεργοποιείται η κάμερα και φωτογραφίζεται το πλαστικό της κάρτας. Η φωτογραφία που λαμβάνεται μέσω του passbook με την εικόνα της κάρτας δεν αποθηκεύετε σε κανένα μέρος της συσκευής παρά μόνο αναγνωρίζεται ο αριθμός της κάρτας και ακολουθεί η αποστολή του κρυπτογραφημένου PAN και της ημερομηνίας λήξης μέσω μιας ασφαλούς σύνδεσης στους servers της Apple. Ακολούθως αποκρυπτογραφούνται στα δεδομένα που παραλήφθηκαν και ανάλογα με τον τύπο της κάρτας αποστέλλεται αίτημα στον κατάλληλο TSP για έκδοση ενός payment token ή του Device Account Number (DAN) σύμφωνα με την ορολογία της Apple. Όλα τα δεδομένα που περιλαμβάνονται στο αίτημα έκδοσης του DAN αποστέλλονται επίσης κρυπτογραφημένα και αφορούν στοιχεία σχετικά με την κίνηση των λογαριασμών iTunes και App Store, στοιχεία της συσκευής όπως ο αριθμός τηλεφώνου, το ονοματεπώνυμο, ο τύπος της συσκευής καθώς επίσης και γεωγραφικά δεδομένα με τις συντεταγμένες της συσκευής την δεδομένη χρονική στιγμή. Ο TSP στη συνέχεια προωθεί το αίτημα στην εκδότρια τράπεζα για ταυτοποίηση και επαλήθευση (ID&V) των στοιχείων της κάρτας. Εφόσον το αποτέλεσμα του ID&V είναι θετικό, τότε ο TSP παράγει το payment token μαζί με την ημερομηνία λήξης του, καθώς και το κλειδί που θα χρησιμοποιείται για την δημιουργία του dynamic security code και αφού τα αποθήκευση σε αντιστοίχιση πάντα με το πραγματικό PAN και την ημερομηνία λήξης του, επιστρέφει τα δεδομένα στην Apple.

Η Apple προωθεί τα στοιχεία του payment token στην συσκευή η οποία εκκίνησε την διαδικασία, χωρίς να κρατήσει καμία πληροφορία ούτε σχετικά με το PAN ούτε με το DAN. Τέλος η συσκευή αποθηκεύει στο SE το DAN, μαζί με την ημερομηνία λήξης και το κλειδί του dynamic security code και έτσι ολοκληρώνετε η διαδικασία προσθήκης μιας κάρτας στην υπηρεσία.



Σχήμα 8: Προσθήκη κάρτας στο Apple Pay

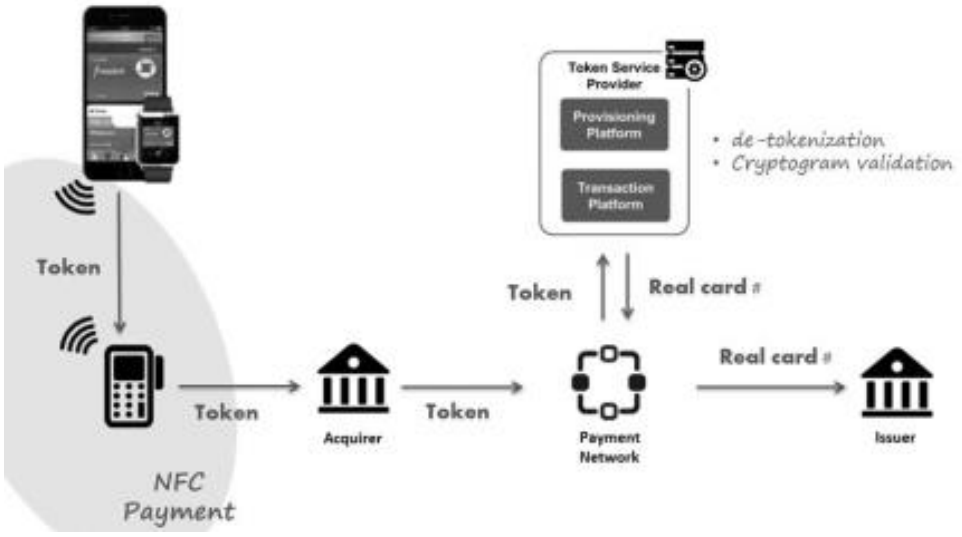
6.5.2 Εκτέλεση πληρωμών

Με την προσθήκη NFC chip στις νέες συσκευές της η Apple, εκτός από τις αγορές μέσω εφαρμογών, η εταιρία επιτυγχάνει να κάνει δυνατή την χρήση του Apple Pay και μέσω καταστημάτων τα οποία διαθέτουν τα γνωστά PoS με contactless αναγνώστες, χωρίς να απαιτείται καμία αναβάθμιση σε αυτά τα συστήματα. Δυστυχώς όμως η υπηρεσία δεν καλύπτει ένα μεγάλο κομμάτι της αγοράς το οποίο συνεχώς αυξάνεται και αφορά τις συναλλαγές μέσω διαδικτύου (eCommerce).

6.5.2.1 Πληρωμές στο κατάστημα (In-Stores)

Η ενσωμάτωση του NFC chip επιτρέπει στις συσκευές να συμπεριφέρονται ως έξυπνες κάρτες κάνοντας χρήση της αντίστοιχης λειτουργίας NFC εξομοίωσης καρτών, όπως αυτό περιγράφεται στα πρότυπα λειτουργίας του πρωτοκόλλου. Όταν επομένως ο καταναλωτής καλείτε να πληρώσει αντί να χρησιμοποιήσει την πλαστική κάρτα μπορεί να πλησιάσει την έξυπνη συσκευή του στην τερματική συσκευή PoS ακριβώς με τον ίδιο τρόπο που θα

έπραττε και με μια φυσική contactless κάρτα. Αμέσως θα εμφανιστεί στην οθόνη του η προεπιλεγμένη κάρτα, σε περίπτωση που έχει πάνω από μια, και ακολούθως θα πρέπει είτε να επιλέξει αυτή την κάρτα ή να επιλέξει κάποια άλλη από τις διαθέσιμες. Η διαδικασία ολοκληρώνεται με την ανάγνωση του δακτυλικού αποτυπώματος, στις συσκευές που διαθέτουν Touch ID, ή με την εισαγωγή του passcode για την επικύρωση της συναλλαγής. Με την χρήση του Apple Pay αντί για την μετάδοση του πραγματικού PAN, η συσκευή αποστέλλει το DAN, όπως αυτό περιεγράφηκε παραπάνω, μαζί με το κρυπτόγραμμα, το οποίο παράγεται και κρυπτογραφείται από το SE, με το κλειδί που έχει λάβει η συσκευή κατά την προσθήκη της κάρτας, λαμβάνοντας ως παραμέτρους διάφορα δεδομένα της συναλλαγής. Το DAN έχει την ίδια μορφή που έχουν και τα PAN, επομένως για την τερματική συσκευή PoS η συναλλαγή αυτή δεν διαφέρει σε τίποτα από μια συναλλαγή με φυσική contactless κάρτα. Αφού ολοκληρωθεί η επεξεργασία της συναλλαγής από το PoS, προωθείται στον αποδέκτη (acquirer) όπως ισχύει και με τις φυσικές κάρτες. Από το BIN του DAN, ο αποδέκτης αναγνωρίζει τον τύπο της κάρτας (Visa, MasterCard, AmEx) και προωθεί τη συναλλαγή στο αντίστοιχο δίκτυο πληρωμών. Το κάθε δίκτυο πληρωμών διαθέτει τον δικό του TSP και αφού αναγνωριστεί ότι η συναλλαγή περιλαμβάνει payment token αντί για PAN στέλνει το DAN μαζί με το κρυπτόγραμμα στο αντίστοιχο σύστημα για επαλήθευση και επιστροφή του PAN. Ο TSP ελέγχει το payment token και το cryptogram και εφόσον είναι έγκυρα τότε εκτελεί την διαδικασία de-tokenisation ανακτώντας το PAN και την ημερομηνία λήξης, τα οποία είναι αποθηκευμένα και συσχετισμένα με το payment token. Στη συνέχεια επιστρέφει το PAN και την ημερομηνία λήξης στο δίκτυο πληρωμών, το οποίο με την σειρά του τα αντικαθιστά και στέλνει προς έγκριση την συναλλαγή στην εκδότρια τράπεζα.

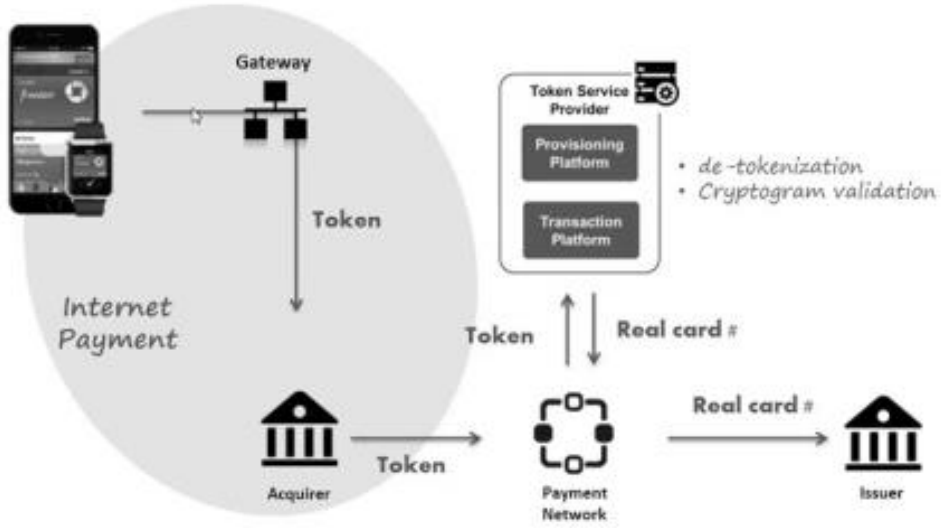


Σχήμα 9: Apple Pay - In stores payments

Για τις συναλλαγές που γίνονται με το Apple Watch, το οποίο δεν διαθέτει Touch ID, η ταυτοποίηση επιτυγχάνεται με το skin sensor όπως έχει επεξηγηθεί στην αντίστοιχη ενότητα.

6.5.2.2 Πληρωμές μέσω εφαρμογής (In-Apps)

Για τις λεγόμενες In-Apps πληρωμές, οι προγραμματιστές πρέπει να έχουν προσθέσει το αντίστοιχο πλήκτρο “Apple Pay” στους διαθέσιμους τρόπους πληρωμής, έχοντας ενσωματώσει και υλοποιήσει στις εφαρμογές τους το Apple Pay API της εταιρίας. Όταν επομένως κάποιος χρήστης επιλέξει αυτόν τον τρόπο πληρωμής, η συσκευή εμφανίζει τις διαθέσιμες κάρτες με τον ίδιο τρόπο που περιεγράφηκε και στις πληρωμές μέσω καταστήματος και αφού στείλει τα δεδομένα της συναλλαγής στο SE, παράγεται το κρυπτόγραμμα. Το κρυπτόγραμμα μαζί με το DAN επιστρέφονται κρυπτογραφημένα στην εφαρμογή για την προώθηση της πληρωμής στον αποδέκτη μέσω της διαθέσιμης σύνδεσης. Αν και από το παρακάτω σχήμα δεν γίνεται απολύτως κατανοητό, ωστόσο στο gateway που μεσολαβεί μεταξύ της συσκευής και του αποδέκτη περιλαμβάνονται και οι servers του Apple Pay, οι οποίοι αναλαμβάνουν την επεξεργασία και την αποστολή των συναλλαγών στον αποδέκτη. Το NCF chip δεν συμμετέχει πουθενά στις In-Apps πληρωμές. Από το σημείο αυτό και μετά η διαδρομή που ακολουθείται και οι ενέργειες που εκτελούνται προκειμένου η συναλλαγή να δρομολογηθεί στην εκδότρια τράπεζα για να λάβει έγκριση είναι οι ίδιες με εκείνες που εφαρμόζονται και στις πληρωμές μέσω καταστήματος.



Σχήμα 10: Apple Pay - In apps payments

6.5.3 Υποστηριζόμενες συσκευές

Για την υποστήριξη του Apple Pay οι συσκευές πρέπει να είναι εξοπλισμένες τουλάχιστον με SE. Όπως φαίνεται και παρακάτω οι συσκευές iPad, οι οποίες διαθέτουν SE chip αλλά δεν διαθέτουν NFC chip, υποστηρίζουν το Apple Pay αλλά μόνο για In Apps πληρωμές. Αντίθετα το Apple Watch το οποίο διαθέτει NFC chip υποστηρίζει το Apple Pay αλλά θα πρέπει να είναι συνεζευγμένο με μια συσκευή iPhone η οποία να διαθέτει SE chip. Παρότι στον πίνακα παρουσιάζεται ότι το Apple Watch υποστηρίζει μόνο πληρωμές In Stores, θεωρητικά θα μπορούσε να υποστηρίξει και In Apps πληρωμές αλλά αυτό είναι μάλλον πρακτικά δύσκολο λόγω των περιορισμών της συσκευής. Τέλος το iPhone 6 το οποίο διαθέτει NFC και SE chips μπορεί να πραγματοποιεί τόσο In Stores συναλλαγές όσο και In Apps.

Products	In Apps	In Stores
iPhone 6 iPhone 6 Plus	✓	✓
Apple Watch Paired with iPhone 5, iPhone 5c, iPhone 5s, iPhone 6, or iPhone 6 Plus.		✓
iPad Air 2 iPad mini 3	✓	

Πίνακας 2: Apple Pay - Συμβατές Συσκευές

6.6 Ασφάλεια και Ιδιωτικότητα

Η Apple έχει δώσει μεγάλη βαρύτητα στα ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας και έχει σχεδιαστεί έτσι η υπηρεσία ώστε να μην μεταδίδονται σε κανένα σημείο της διαδρομής μη κρυπτογραφημένα δεδομένα όπως είναι τα στοιχεία της κάρτας, η ημερομηνία λήξης, το ονοματεπώνυμο του κατόχου κ.α.

Κατά την διάρκεια προσθήκης μιας κάρτας, τα στοιχεία αποστέλλονται στην Apple κρυπτογραφημένα, η εταιρία τα αποκρυπτογραφεί και τα προωθεί στο ανάλογο σύστημα

αφού πρώτα τα κρυπτογραφήσει ξανά και χωρίς προηγουμένως να αποθηκεύσει οποιαδήποτε πληροφορία στα συστήματα της.

Όταν η συσκευή λάβει το DAN το οποίο έχει αντικαταστήσει το PAN, η πληροφορία αυτή είναι κρυπτογραφημένη και αποθηκεύεται επίσης κρυπτογραφημένη στο SE, στο οποίο η πρόσβαση είναι απόλυτα ελεγχόμενη και περιορισμένη. Επιπλέον ο αριθμός που αποθηκεύεται στο SE είναι το DAN και όχι το PAN επομένως δεν υπάρχει στην συσκευή πλέον καμία σύνδεση με τον πραγματικό αριθμός της κάρτας.

Όταν πραγματοποιείται μια συναλλαγή σε κατάστημα, κάνοντας χρήση της NFC τεχνολογίας, δεν αποστέλλονται τα πραγματικά στοιχεία της κάρτας αφού άλλωστε δεν τα γνωρίζει καν η συσκευή αλλά αντιθέτως αποστέλλετε το DAN, το οποίο δεν μπορεί από μόνο του να χρησιμοποιηθεί αφού απαιτείται και το dynamic security code, το οποίο είναι μοναδικό και μπορεί να χρησιμοποιηθεί μόνο για μια φορά. Επιπλέον για την αποστολή των στοιχείων του DAN στην τερματική συσκευή PoS, θα πρέπει ο χρήστης να δώσει είτε το δακτυλικό του αποτύπωμα είτε το passcode. Επίσης τα στοιχεία των συναλλαγών δεν στέλνονται στην Apple, επομένως δεν μπορεί να γνωρίζει η εταιρία τι συναλλαγές, με τι ποσά και σε ποιες επιχειρήσεις έχουν πραγματοποιηθεί αγορές από τον χρήστη.

Στις συναλλαγές που πραγματοποιούνται μέσω των εφαρμογών τα στοιχεία του DAN μεταβιβάζονται κρυπτογραφημένα στην εφαρμογή που τα έχει ζητήσει χρησιμοποιώντας το δικό της κλειδί έτσι ώστε καμία άλλη εφαρμογή (π.χ. κακόβουλη) να μην μπορεί να έχει πρόσβαση σε αυτά τα δεδομένα. Η Apple κρατάει ανώνυμα δεδομένα με ορισμένα μόνο στοιχεία των συναλλαγών για την βελτίωση του Apple Pay αλλά και άλλων προϊόντων και υπηρεσιών της εταιρίας [2].

Τέλος στην περίπτωση που η συσκευή χαθεί ή κλαπεί, παρόλο που δεν θα μπορούσε κάποιος να χρησιμοποιήσει το Apple Pay αφού πρέπει να δώσει το passcode ή το δακτυλικό αποτύπωμα, ωστόσο η Apple έχει προσθέσει ένα ακόμα μέτρο προστασίας μέσω της υπηρεσίας Find My iPhone. Όταν μια συσκευή τεθεί μέσω του Find My iPhone σε κατάσταση απώλειας, τότε η υπηρεσία του Apple Pay απενεργοποιείται προσωρινά. Αν η συσκευή δεν βρεθεί ή αν αυτή έχει κλαπεί τότε με την επιλογή «Σβήσιμο συσκευής», η Apple προχωράει άμεσα στην ακύρωση των καρτών από το Apple Pay και αν η συσκευή είναι online διαγράφονται όλα τα στοιχεία από αυτήν συμπεριλαμβανομένων των στοιχείων των καρτών. Αν η συσκευή δεν είναι online η διαδικασία της διαγραφής θα εκκινήσει αμέσως μόλις αυτή τεθεί ξανά σε online κατάσταση.

6.7 Αδυναμίες

Παρόλο που ο σχεδιασμός της υπηρεσίες δεν παρουσιάζει αδυναμίες που να θέτουν σε κίνδυνο την ασφάλεια και την ιδιωτικότητα των πραγματικών κατόχων, ωστόσο ο τρόπος εγγραφής των καρτών στην υπηρεσία δίνει την δυνατότητα προσθήκης κάρτας, η οποία μπορεί να μην ανήκει στον κάτοχο της συσκευής. Η συγκεκριμένη αδυναμία όμως φαίνεται να είναι αποδεκτή τόσο από την Apple όσο και από τις τράπεζες διότι πρώτον ο συγκεκριμένος τρόπος καθιστά εύκολη την διαδικασία εγγραφής και μπορεί έτσι να αυξήσει σύντομα την χρήση της υπηρεσίας και δεύτερον δεν οδηγεί σε μεγάλης κλίμακας απάτη. Ο λόγος που δεν οδηγεί σε μεγάλης κλίμακας απάτη είναι διότι αυτοί που διαθέτουν στοιχεία καρτών από το λεγόμενο Cross-Channel Fraud, θα προτιμήσουν μάλλον άλλα κανάλια τα οποία όχι μόνο προσφέρουν περισσότερη ανωνυμία αλλά επιτρέπουν και ευρύτερη χρήση για αγορά υπηρεσιών και αγαθών, όπως είναι για παράδειγμα το eCommerce.

Ορισμένες τράπεζες έχουν λάβει ήδη μέτρα για την αποτροπή εγγραφής καρτών από μη εξουσιοδοτημένα πρόσωπα, επικοινωνώντας για επιβεβαίωση με τους πραγματικούς κατόχους των καρτών μόλις λάβουν ένα ID&V αίτημα για εγγραφή στην υπηρεσία.

Ορισμένες πιθανές αδυναμίες θα μπορούσαν επίσης να είναι κάποιες από τις αδυναμίες της contactless τεχνολογίας όπως για παράδειγμα το relay attack αλλά η χρήση του DAN αντί για το PAN σε συνδυασμό με το dynamic security code καθιστούν μάλλον αδύνατη τη συγκεκριμένη επίθεση.

Η χρήση του Touch ID θα μπορούσε επίσης να αποτελέσει ένα αδύναμο σημείο, διότι όπως ισχυρίζεται η biometrics hacking team του Chaos Computer Club (CCC), έχει επιτύχει να παρακάμψει την ασφάλεια του Apple Touch ID, φωτογραφίζοντας το δακτυλικό αποτύπωμα από μια γυάλινη επιφάνεια και δημιουργώντας αντίγραφο του αποτυπώματος σε λάτεξ υλικό, το οποίο στην συνέχεια χρησιμοποιήσαν αντί του πραγματικού αποτυπώματος [13].

Ούτε η συγκεκριμένη όμως τεχνική μπορεί να χρησιμοποιηθεί για απάτες μεγάλης κλίμακας, καταδεικνύει ωστόσο την δυνατότητα παράκαμψης των ισχυρών, κατά τα άλλα μέτρων προστασίας, τα οποία έχουν εφαρμοστεί για την αποτροπή μη εξουσιοδοτημένης χρήσης.

7. Διαφορετικές υλοποιήσεις

Εκτός από την Apple και άλλες εταιρίες έχουν παρουσιάσει την δικές του λύσεις για πληρωμές με τραπεζικές κάρτες με τη χρήση φορητών έξυπνων συσκευών, κυρίως έξυπνων τηλέφωνων. Ορισμένες από αυτές είχαν κάνει την παρουσία τους πριν από το Apple Pay, ενώ κάποιες άλλες παρουσιάστηκαν αργότερα. Αυτό που είναι φανερό είναι πως παρόλο που η Apple άργησε πολύ να παρουσιάσει μια δική της λύση με την χρήση της τεχνολογίας NFC, ωστόσο πέτυχε η υλοποίηση που τελικά υιοθέτησε όχι μόνο να διαφέρει σημαντικά από τις υπόλοιπες αλλά και να ορίσει τα πλαίσια στα οποία θα κινηθούν και οι επόμενες.

	Apple Pay	**Android Pay**	**Samsung Pay**
Τεχνολογία	NFC	NFC	NFC, MST
Τρόποι Αποδοχής	PoS with CTLS, In Apps	PoS with CTLS, In Apps	All PoS
Ασφάλεια	embedded SE, Tokenisation	HCE, Tokenisation	embedded SE, Tokenisation
Συσκευές	iPhone 6, iPhone 6 Plus Apple Watch paired with an iPhone iPad 2 Air, iPad mini 3	All android devices with KitKat 4.4 and higher	Galaxy 6 Galaxy 6 Edge
Τράπεζες	>500	Citi Group	Bank of America, Chase, Citi Group, US Bank
Τύποι καρτών	Visa, MasterCard, AmEx	MasterCard	Visa, MasterCard, AmEx
Σημεία Αποδοχής	220.000	220.000	Παντού
Έναρξη	Οκτώβριος 2014	Σεπτέμβριος 2015	Καλοκαίρι 2015

Πίνακας 3: Συγκριτικά στοιχεία συστημάτων πληρωμών

7.1 Android Pay

Το Android Pay είναι η δεύτερη λύση πληρωμών που παρουσιάζει η Google μετά το Google Wallet, το οποίο δεν κατάφερε να αποκτήσει κάποιο σημαντικό μερίδιο της αγοράς. Το Android Pay βασίζεται επίσης στην τεχνολογία του tokenization και του NFC όπως και το Apple Pay, με την διαφορά ότι τα στοιχεία των payment tokens δεν αποθηκεύονται σε SE της συσκευής αλλά φυλάσσονται σε κεντρικά συστήματα της εταιρίας κάνοντας χρήση της

τεχνικής Host Card Emulation (HCE). Το πλεονέκτημα αυτής της υλοποίησης είναι ότι μπορεί να υποστηριχθεί από οποιαδήποτε android συσκευή διαθέτει NFC chip χωρίς όμως να απαιτείται και ενσωματωμένο SE.

7.2 Samsung Pay

Η πρόταση της εταιρίας Samsung είναι πολύ ενδιαφέρουσα αφού εκτός από τις κλασσικές πλέον υλοποιήσεις με χρήση του tokenisation σε συνδυασμό με την τεχνολογία NFC, η εταιρία προσθέτει ακόμα μια τεχνική, η οποία ονομάζεται Magnetic Secure Transmission (MST) και στην πράξη εξομοιώνει την λειτουργία μιας μαγνητικής κάρτας όταν αυτή περνάει από τον μαγνητικό αναγνώστη ενός PoS. Η λογική πίσω από αυτή την τεχνική είναι αντίστοιχη με αυτή του NFC σε λειτουργία εξομοίωσης καρτών. Το πλεονέκτημα της υιοθέτησης αυτής της τεχνικής είναι ότι η συσκευή μπορεί να λειτουργήσει σε όλα τα σημεία αποδοχής καρτών, ανεξάρτητα από το αν αυτά διαθέτουν contactless αναγνώστη ή όχι. Μοναδική εξαίρεση αποτελούν οι unattended συσκευές οι οποίες για να διαβάσουν την μαγνητική πίστα μιας κάρτας πρέπει να γίνει εισαγωγή τους σε ειδική υποδοχή (π.χ. ATM). Το Samsung Pay επίσης κάνει χρήση ενσωματωμένου SE για την αποθήκευση των payment tokens.

7.3 CurrentC

Το Merchant Customer Exchange (MCX) κονσόρτσιουμ, το οποίο αποτελείται από περισσότερες από 50 μεγάλες αλυσίδες λιανικής στην Αμερική, όπως είναι το WalMart, η Target Corporation, το Bust Buy, η GAP και πολλές άλλες ακόμα, ανάπτυξαν τον τρόπο πληρωμής CurrentC, ο οποίος βασίζεται στις αρχές του tokenization. Οι πληρωμές γίνονται μέσω εφαρμογής που πρέπει να εγκαταστήσει ο κάτοχος ενός έξυπνου τηλεφώνου στη συσκευή και να εγγραφεί στην συγκεκριμένη υπηρεσία δηλώνοντας τις κάρτες του. Τα στοιχεία των καρτών φυλάσσονται κεντρικά σε συστήματα της MCX και η πληρωμή γίνεται είτε με την ανάγνωση ενός QR code που εμφανίζεται στην οθόνη της ταμειακής, είτε με QR που παράγεται από την εφαρμογή του κινητού, το οποίο δίνεται για ανάγνωση στο ταμειακό σύστημα του εμπόρου. Το QR code αποστέλλεται στα συστήματα της MCX, τα οποία λαμβάνουν όλα τα στοιχεία της συναλλαγής (έμπορος, κάρτα χρέωσης, ποσό κ.α.) και μέσω ενός δικτύου πληρωμών που ονομάζεται Automated Clearing House (ACH), προωθεί το αίτημα στην εκδότρια τράπεζα προς έγκριση.

Συμπεράσματα

Η καθυστερημένη υιοθέτηση της τεχνολογίας του NFC από την Apple οδήγησε, όπως αναμενόταν από πολλούς κύκλους της αγοράς, στην παρουσίαση μιας νέας τεχνολογικής λύσης, η οποία να διαφέρει σημαντικά με ότι ήταν γνωστό μέχρι τότε. Η υπηρεσία Apple Pay είναι ο νέος τρόπος πληρωμής που σχεδιάστηκε και αναπτύχθηκε από την Apple, αξιοποιώντας αποτελεσματικά υπάρχουσες σύγχρονες τεχνολογίες όπως είναι το NFC και το tokenisation. Η πρόταση της Apple πέτυχε όχι μόνο να γίνει άμεσα ευρέως αποδεκτή από την αγορά αλλά και να ορίσει τελικά το πλαίσιο στο οποίο θα κινηθούν και όλες οι νέες υλοποιήσεις που θα ακολουθήσουν.

Ένας σημαντικός περιορισμός του Apple Pay αφορά τους τρόπους αποδοχής της υπηρεσίας που υποστηρίζει μόνο τις πληρωμές μέσω των φυσικών καταστημάτων τα οποία διαθέτουν PoS με contactless και των iOS εφαρμογών. Οι ηλεκτρονικές πληρωμές που γίνονται στο διαδίκτυο μέσω εφαρμογών περιήγησης δεν υποστηρίζονται από αυτή την υπηρεσία. Επειδή όμως οι συγκεκριμένες συναλλαγές αποτελούν ένα αρκετά σημαντικό κομμάτι στο μερίδιο της αγοράς, το οποίο συνεχώς αυξάνετε, αναμένονται με ενδιαφέρον οι επόμενες να κινήσεις της εταιρίας.

Η εφαρμογή ισχυρών τεχνολογικών λύσεων όπως είναι το SE, για την αποθήκευση των στοιχείων των καρτών και των κλειδιών αλλά και το tokenisation, για την αντικατάσταση του PAN με ένα payment token, έχουν συνδυαστεί με ένα αρκετά αποτελεσματικό τρόπο, προσφέροντας ένα σύγχρονο και ασφαλή τρόπο πληρωμής. Η υλοποίηση του tokenisation από το Apple Pay είναι απόλυτα συμβατή με τις προδιαγραφές που έχει θέσει το EMVco.

Όταν γίνεται προσθήκη μιας κάρτας στη συσκευή, όλα τα στοιχεία μεταφέρονται κρυπτογραφημένα και η Apple δεν κρατάει κανένα στοιχείο στα συστήματα της. Το αποτέλεσμα της προσθήκης μιας κάρτας στην υπηρεσία είναι η μετατροπή του PAN σε ένα άλλο λογαριασμό με την ονομασία DAN, ο οποίος αποθηκεύεται κρυπτογραφημένος σε ασφαλές μέρος της συσκευής (eSE). Οι συναλλαγές που εκτελούνται, αφού έχει προηγηθεί η προσθήκη καρτών στη συσκευή, πραγματοποιούνται με την χρήση του DAN, επομένως ούτε ο έμπορος αλλά ούτε και η Apple γνωρίζουν το πραγματικό PAN. Ακόμα και αν καταφέρει κάποιος να υποκλέψει τα στοιχεία του DAN, δεν θα μπορέσει να τα χρησιμοποιήσει για να κάνει αγορές από άλλα κανάλια (π.χ. eCommerce), αφού το DAN συνδυάζεται πάντα με ένα δυναμικό security code το οποίο είναι μιας χρήσης, σε αντίθεση με το CVV του PAN που είναι στατικό.

Παρόλο που η χρήση του Apple Pay διαθέτει ορισμένα αδύναμα σημεία, τα οποία θα μπορούσε κάποιος να αξιοποιήσει για να εκτελέσει πληρωμές χωρίς εξουσιοδότηση, τελικά οι ενέργειες που μπορεί να κάνει είναι περιορισμένες και δεν οδηγούν σε μεγάλης κλίμακας απάτη. Πράγματι στους πρώτους μήνες λειτουργίας της υπηρεσίας στην Αμερική δεν έχουν παρουσιαστεί απάτες αυτού του είδους, όμως όσο η αποδοχή της υπηρεσίας θα αυξάνεται, τόσο περισσότερο θα στρέφεται και η προσοχή του οργανωμένου οικονομικού εγκλήματος προς αυτή την κατεύθυνση.

Βιβλιογραφία

1. Apple Pay, “Your Wallet. Without the Wallet.”, Apple, 2015, [Online]. Available: https://www.apple.com/apple-pay/
2. Apple Pay, “Apple Pay security and privacy overview”, Apple. 2015, [Online]. Available: https://support.apple.com/en-us/HT203027
3. EMVCo, "Payment Tokenisation Specification - Technical Framework", EMVCo LLC, 2014, [Online]. Available: https://www.emvco.com/download_agreement.aspx?id=945
4. Scoping SIG, Tokenization Taskforce PCI Security Standards Council, "Information Supplement: PCI DSS Tokenization Guidelines", PCI Security Standards Council, 2011, [Online], Available: https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf
5. UL, "Tokenization Explained: What it is, how it works and how you can benefit", 2015, [Online], Available: https://www.ul-ts.com/use-cases/tokenization/white-papers-and-case-studies/tokenization-explained/c-37/c-2054/p-1622
6. UL, “Apple Pay – What do we know?”, 2014, [Online], Available: http://www.planetbiometrics.com/creo_files/upload/article-files/apple_pay_-_what_do_we_know.pdf
7. PhD Francisco Corella, MD Karen Lewison, "Interpreting the EMV Tokenisation Specification", October, 2014, [Online]. Available: http://pomcor.com/whitepapers/EMVTok.pdf
8. Michael Roland, Josef Langer, "Cloning Credit Cards: A combined pre-play and downgrade attack on EMV Contactless", NFC Research Lab Hagenberg, University of Applied Sciences Upper Austria, 2012
9. First Data Corporation, "EMV and Encryption + Tokenization: A Layered Approach to Security", 2012, [Online]. Available: http://www.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF
10. Apple, “Getting Started with Passbook on iOS 6”, [Online]. Available: https://developer.apple.com/passbook/Getting_Started_with_Passbook.pdf

11. Apple, “About Touch ID security on iPhone and iPad”, [Online]. Available: https://support.apple.com/en-us/HT204587

12. Wikipedia, “Bank card number”, [Online]. Available: https://en.wikipedia.org/wiki/Bank_card_number

13. CCC, “Chaos Computer Club breaks Apple TouchID”, [Online]. Available: http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

14. Smartcard, “Smart Card Tutorial - Part 1”, [Online]. Available: http://www.smartcard.co.uk/tutorials/sct-itsc.pdf

15. Apple, “Find My iPhone, iPad, iPod touch, or Mac”, Online]. Available: https://www.apple.com/support/icloud/find-my-iphone-ipad-ipod-mac/

16. Wiki, “Merchant Customer Exchange”, [Online]. Available: https://en.wikipedia.org/wiki/Merchant_Customer_Exchange

17. TSYS, “Tokenization: FAQs & General Information”, [Online]. Available: http://tsys.com/Assets/TSYS/downloads/br_tokenization-faqs-and-general-information.pdf

18. TechTarget, “What Apple Pay tokenization means for PCI DSS compliance”, [Online]. Available: http://searchsecurity.techtarget.com/tip/What-Apple-Pay-tokenization-means-for-PCI-DSS-compiance

19. Mobiquity Inc, “Apple Pay: How It Works”, [Online]. Available: https://www.mobiquityinc.com/apple-pay-how-works

20. NFC Forum, “About the Technology, NFC and Contactless Technologies”, [Online]. Available: http://nfc-forum.org/what-is-nfc/about-the-technology/