Πανεπιστήμιο Πειραιά

Τεχνική Ανάλυση Mobile Wallets και Συστημάτων Πληρωμών

Τμήμα Ψηφιακών Συστημάτων

Κωνσταντόπουλος Γεώργιος

MTE 1320

Πειραιάς, Γενάρης 2016

Ευχαριστίες

Η παρούσα διπλωματική εργασία αποτελεί προϊόν εκτενούς μελέτης και έρευνας πάνω σε ένα σύγχρονο και απαιτητικό αντικείμενο. Με το παρόν, θα ήθελα να ευχαριστήσω θερμά τον επιβλέπων καθηγητή μου κ. Λαμπρινουδάκη Κωνσταντίνο, για την καθοριστική του συμβολή και καθοδήγηση σε όλη την διάρκεια της εκπόνησης της εργασίας.

Ευχαριστώ επίσης και τους κ.κ. Ξενάκη Χρήστο και Νταντογιάν Χ. για την παρουσία και συμμετοχή τους στην τριμελή επιτροπή μου. Φυσικά, δεν θα μπορούσα να μην ευχαριστήσω την οικογένεια μου για την στήριξη και κυρίως την υπομονή τους αυτό το διάστημα!

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Ακρωνύμια

API:	Application Programming Interface
AR:	Authorization Value
ARPC:	Authorization Response Cryptogram
ARQC:	Authorization Request Cryptogram
ATM:	Automated Teller Machine
AES:	Advanced Encryption Standard
BIN:	Bank Identification Number
BLE:	Bluetooth Low Energy
CA:	Certificate Authority
CCM:	Client Certificate Management
CCN:	Credit Card Number
CTR_DRBG:	Counter Mode Deterministic Random Byte Generator
CVM:	cardholder verification method
CVV:	Card Verification Value
DAN:	Device Account Number
DUHK:	Device Unique Hardware Key
DDA:	Dynamic Data Authentication
DOS:	Denial of Service
DRK:	Device Root Key
DSS:	Data Security Standard
EER:	Equal Error rate
EMVCo:	Europay, Mastercard and Visa Corporation
E2EE:	End to End Encryption
FAR:	False Accept Rate
FRR:	False Reject Rate
FTC:	Failure to Capture
FTE:	Failure to Enroll
GAP:	Generic Access Profile
HCE:	Host Card Emulation
HCI:	Host to Controller Interface
HSM:	Hardware Security Module
ICC:	Integrated Circuit Card
INN:	Issuer Identification Number
ISM:	Industrial, Scientific and Medical (radio Bands)
MB-ME:	Message Begins-Message Ends
MNO:	Mobile Network Operators
MSR:	Magnetic Stripe Reader
MST:	Magnetic Secure Transmission
Ndef:	NFC Data Exchange Format
NFC:	Near Field Communication
OEM:	Original Equipment Manufacturer
OTA:	Over the Air
PAN:	Primary Account Number

PAN:	Personal Area Network
PBL:	Primary Bootloader
PCD:	Proximity Coupling Device
PCI:	Payment Card Industry
PICC:	Proximity IC Card
PII data:	Personally identifiable information
PIN:	Personal Identification Number
POS:	Point of Sale
P2P:	Peer to Peer
P2PE:	Point to Point Encryption
QR:	Quick Response
RF:	Radio Frequency
RFID:	Radio Frequency Identification
ROC:	Receiver Operating Characteristic
RP Fuse:	Roll Back Fuse
SDA:	Static Data Authentication
SHA-1:	Secure Hash Algorithm
SE:	Secure Element
SIM:	Subscriber Identity Module
SPI:	Serial Peripheral Interface
SSBK:	Samsung Secure Boot Key
SSL:	Secure Socket Layer
SSN:	Social Security Number
TEE:	Trust Execution Environment
TIMA:	TrustZone-Based Integrity Measurement Architecture
TR:	Token Requestor
TSP:	Token Service Provider
UID:	Unique ID
URL:	Uniform Resource Locator
VAN:	Virtual Account Number
VAS:	Value Added Service
3DS:	Three Domain Secure

Εισαγωγή

Τον Σεπτέμβριο του 1958, η Bank of America κυκλοφόρησε την BankAmericard, την πρώτη επιτυχημένη, πιστωτική κάρτα στον δυτικό κόσμο. Η κίνηση αυτή σηματοδότησε την αρχή για μια μεγάλη αλλαγή στον τρόπο διαχείρισης μετρητών και τον τρόπο που πραγματοποιούνται οι συναλλαγές. Τα τελευταία χρόνια όμως, είμαστε στις αρχές μίας ακόμα μεγάλης αλλαγής στον τρόπο με τον οποίο εκτελούνται οι συναλλαγές. Η τεράστια εξέλιξη στον χώρο της κινητής τηλεφωνίας και η αποδοχή που έχει από το καταναλωτικό κοινό, έδωσε το έναυσμα για την δημιουργία ενός νέου μοντέλου διαχείρισης των καρτών και πληρωμών, τα "Ψηφιακά Πορτοφόλια" ή αλλιώς, Mobile Wallets. Ως Mobile Wallet ορίζουμε το καινούργιο σύστημα συναλλαγών το οποίο προσφέρει μία πλατφόρμα πάνω σε κινητές συσκευές με έντονα στοιχεία ασφάλειας και κρυπτογραφίας, ώστε να αποθηκεύονται εκεί κάρτες τραπεζικών φορέων, με σκοπό να πραγματοποιούνται συναλλαγές τόσο εντός καταστήματος όσο και online απουσία των φυσικών καρτών.

Χρησιμοποιούνται και άλλες ορολογίες όπως Digital Wallet, e-Wallet, Smart Wallet, αλλά για τις ανάγκες αυτής της μελέτης θα προτιμηθεί ο όρος Mobile Wallet καθώς περιγράφει καλύτερα το κομμάτι των συναλλαγών πάνω στο οποίο δίνει βάση. Με τις υπόλοιπες ορολογίες θα ήταν δυνατό να οριστεί μία πιο ολοκληρωμένη λύση η οποία θα αποτελούσε τον αντικαταστάτη του κλασσικού πορτοφολιού με την μορφή που το ξέρουμε τώρα, το οποίο πέρα από τις χρεωστικές και πιστωτικές κάρτες, θα περιείχε και στοιχεία ταυτότητας, διπλώματος

οδήγησης, εισιτήρια συγκοινωνιών και ότι άλλο θα έβρισκε κάποιος μέσα σε ένα κανονικό πορτοφόλι.

Σκοπός αυτής της έρευνας, είναι να αναλυθεί ο τρόπος λειτουργίας των Mobile Wallets, κάνοντας εκτενή αναφορά σε βασικές αλλά και σύνθετες τεχνολογίες πάνω στις οποίες στηρίζονται και ερευνώντας τις μεθοδολογίες τις οποίες έχουν υιοθετήσει, μέχρι αυτή την στιγμή στην αγορά, οι μεγαλύτεροι οργανισμοί που υλοποιούν λύσεις Mobile Wallet, δίνοντας περισσότερο βάση στην ασφάλεια που προσφέρει η κάθε πλατφόρμα.

Στο 1ο κεφάλαιο γίνεται εκτενής αναφορά στον τρόπο λειτουργίας του τραπεζικού συστήματος και συστημάτων πληρωμών, όπως επίσης και στην έννοια του tokenization, καθώς αποτελεί το συνολικό οικοσύστημα μέσα στο οποίο αναπτύχθηκε αυτό το καινούργιο μοντέλο πληρωμών. Στο 2ο κεφάλαιο, παρουσιάζεται διεξοδικά το σύνολο των τεχνολογιών που αποτελούν το παρών αλλά και το μέλλον για τις υλοποιήσεις των mobile wallets. Στο 3ο κεφάλαιο, παρουσιάζεται συνοπτικά ένα σύνολο απειλών που σχετίζονται με τα mobile wallets. Στα κεφάλαια 4 έως και 7 παρουσιάζονται οι υλοποιήσεις των Mobile Wallets οι οποίες σύμφωνα με τα τωρινά δεδομένα, θα απασχολήσουν το μεγαλύτερο ποσοστό της αγοράς τα επόμενα χρόνια. Συνολικά θα γίνει ανάλυση τεσσάρων case studies, Apple Pay, Samsung Pay, Android Pay και Wocket, η οποία και αποτελεί την μοναδική stand alone υλοποίηση (δεν κάνει χρήση τηλεφωνικής συσκευής). Τέλος, μέσα από συγκρίσεις και παρατηρήσεις, παρουσιάζονται συμπεράσματα (αποδοχή του προϊόντος, ασφάλεια) και προτάσεις για το πώς θα πρέπει να κινηθεί στο μέλλον εξασφαλίζοντας περισσότερη ασφάλεια για τους χρήστες αυτών των υπηρεσιών.

1. Τραπεζικό Μοντέλο Συναλλαγών με Κάρτα

1.1. Εισαγωγή

Για να γίνει αντιληπτός καλύτερα ο τρόπος λειτουργίας ενός Mobile Wallet, πρέπει να γίνει αναφορά στο σύστημα πληρωμών και συναλλαγών πάνω στο οποίο αναπτύχθηκε και την σχέση μεταξύ πελάτη, εμπόρου και χρηματοπιστωτικού συστήματος. Οι τράπεζες στην Ευρώπη έχουν πραγματοποιήσει ήδη μια μεγάλη αλλαγή υιοθετώντας τις κάρτες τεχνολογίας EMV, σε μια προσπάθεια να αλλάξουν τον «χάρτη της απάτης» όπως αυτός είχε διαμορφωθεί. Η Αμερική άργησε αλλά ακολούθησε, με το λεγόμενο Liability Shift να ισχύει από το Οκτώβριο του 2015, με το οποίο "εξανάγκασε" τους εμπόρους να αναβαθμίσουν τα τερματικά τους POS σε EMV enabled POS, καθώς όσοι δεν συμμορφώνονταν με την αλλαγή, σε περίπτωση απάτης με κάρτα κατά την διάρκεια πληρωμής στην επιχείρησή τους, η υπαιτιότητα θα ήταν εις βάρος του εμπόρου και του Acquirer (1)

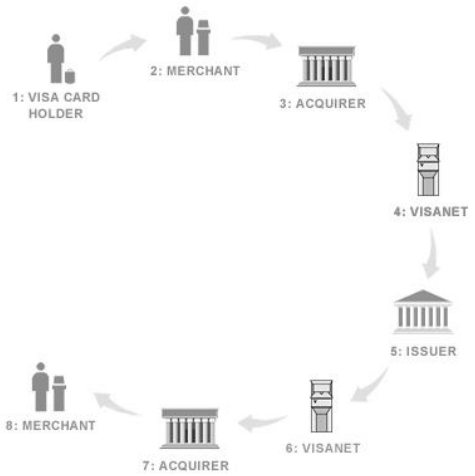
1.2. Πως πραγματοποιείται μία συναλλαγή

Σε μία τυπική συναλλαγή σε μία επιχείρηση, εμπλέκονται οι παρακάτω οντότητες (2): ο **Cardholder** (ο κάτοχος της κάρτας), ο **Issuer** (η τράπεζα που έχει εκδώσει την αντίστοιχη Visa/Mastercard στον Cardholder), ο **Merchant** (έμπορος), ο **Acquirer** (η τράπεζα που συνεργάζεται με τον Merchant) και το **Payment Network** (γενικός όρος, που περιγράφει το Payment network που βρίσκεται πίσω από την κάρτα, πχ Visa ή Mastercard). Στο σχήμα που περιγράφεται, αφήνονται εσκεμμένα εκτός τυχόν 3rd party token providers. Μία απλή συναλλαγή σε κατάστημα με χρήση κάρτας περιγράφεται παρακάτω. Η διαδικασία περιλαμβάνει δύο κύκλους εργασιών :

1. Το **authorization** και

2. Το **clearing & settlement**.

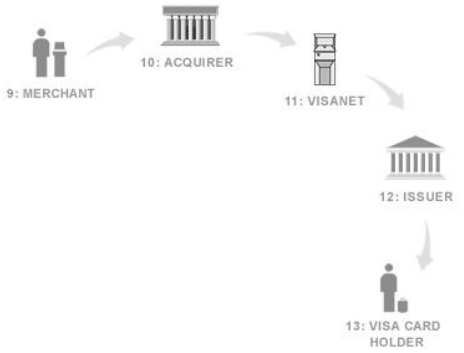
Στον 1ο κύκλο, συναντώνται τα παρακάτω βήματα**(εικόνα_1)**,



Εικόνα 1 Κύκλος authorization, Visa Canada

1. Ο cardholder παρουσιάζει την κάρτα στο κατάστημα
2. Ο merchant περνάει την κάρτα από το τερματικό, εισάγει το προς χρέωση ποσό και προωθεί ένα αίτημα για έγκριση της συναλλαγής στον Acquirer
3. Ο Acquirer προωθεί το αίτημα στο Payment network
4. Το Payment Network στέλνει με τη σειρά του το αίτημα στον Issuer του Cardholder
5. Ο Issuer εγκρίνει ή απορρίπτει τη συναλλαγή και αποστέλλει απάντηση στο Payment Network.
6. Το Payment network στέλνει την απάντηση στον Acquirer του merchant
7. Ο Acquirer ενημερώνει ηλεκτρονικά τον Merchant
8. Ο Merchant λαμβάνει την απάντηση από την απόφαση του Issuer και εάν είναι θετική, προχωρά στην ολοκλήρωση της συναλλαγής.

Στον 2ο κύκλο έχουμε τα εξής βήματα, με τα οποία ολοκληρώνεται η διαδικασία της συναλλαγής**(εικόνα_2)**.



Εικόνα 2 Κύκλος Clearing & Settlement, Visa Canada

9. Ο Merchant καταθέτει την "απόδειξη" της συναλλαγής στον Acquirer με τον οποίο συνεργάζεται.
10. Ο Acquirer πιστώνει τον λογαριασμό του Merchant και προωθεί ηλεκτρονικά την συναλλαγή στο payment Network για εκκαθάριση.
11. Το Payment network, πληρώνει τον Acquirer, πιστώνει τον λογαριασμό του Issuer και τέλος προωθεί την συναλλαγή στον Issuer
12. Ο Issuer εμφανίζει την συναλλαγή στον λογαριασμό του cardholder και τον ενημερώνει στον μηνιαίο report.
13. Ο Cardholder χρεώνεται στο λογαριασμό του και ολοκληρώνεται η διαδικασία με την ενημέρωση του από το μηνιαίο report.

1.3. Πως λειτουργεί το Tokenization στο σύγχρονο τραπεζικό σύστημα

Στην επιστήμη της Ασφάλειας Δεδομένων, **Tokenization** είναι η διαδικασία με την οποία γίνεται αντικατάσταση ενός ευαίσθητου δεδομένου με ένα μη-ευαίσθητο, το οποίο ονομάζεται **token** και το οποίο δεν έχει καμία αξία για απάτη ή εκμετάλλευση. Η αντιστοίχιση του token με τα πραγματικά δεδομένα, γίνεται με διαδικασίες που κάνουν την εύρεση τους ασύμφορη από άποψη πόρων.

Είναι σημαντικό να τονιστεί ότι το tokenization είναι μια διαδικασία επικουρική αλλά διαφορετική του encryption. Το tokenization αλλάζει μεν το PAN με ένα τυχαίο "νούμερο" αλλά δεν υπάρχει τρόπος για κάποιον που το έχει στην κατοχή του με υποκλοπή να φτάσει στο πραγματικό PAN με κάποια συνάρτηση. Το encryption από την άλλη, στηρίζεται σε

συγκεκριμένους αλγόριθμους και κλειδιά για να κρυπτογραφήσει το token και τα υπόλοιπα δεδομένα του μηνύματος καθιστώντας πού δύσκολη την αποκρυπτογράφηση του χωρίς τα αντίστοιχα κλειδιά και γνώση των αλγορίθμων.

Μέχρι και πρόσφατα, το tokenization το χρησιμοποιούσαν για να προστατέψουν data-at-rest, δηλαδή δεδομένα που δεν συμμετέχον άμεσα σε κάποια συναλλαγή, πχ δεδομένα σε μια βάση δεδομένων όπως τον αριθμό της κάρτας, όπου εξυπηρετούσε τους Merchants για back-end λειτουργίες όπως επιστροφές χρημάτων, loyalty υπηρεσίες, κα. Με την αύξηση όμως της απάτης στην διάρκεια των συναλλαγών, δημιουργήθηκε η ανάγκη για πιο άμεση προστασία σε όλο το φάσμα της συναλλαγής (end-to-end). Θα γίνει αναφορά στον τρόπο λειτουργίας των tokens, την συμμετοχή της **EMVCo**, και τον ρόλο των **Token Service Providers** (**TSP**).

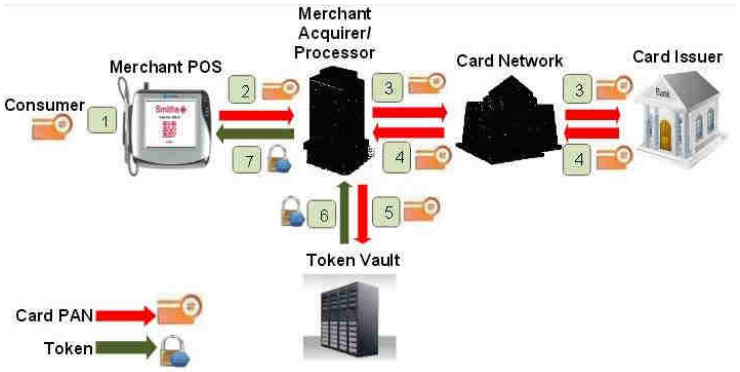
Τα tokens στο χώρο του εμπορίου και των συναλλαγών (3), ανέπτυξαν δύο ρόλους και αντίστοιχα δύο διαφορετικούς τρόπους λειτουργίας,

1. **Security** (ή Acquirer) token και

2. **Payment** (ή Issuer) token.

Οι δεύτερες ονομασίες τους εντός των παρενθέσεων κάνουν σαφή και τον προσανατολισμό τους με τα Security tokens να είναι πιο Merchant-oriented. Τα Security tokens,έχουν σκοπό να αντικαταστούν ευαίσθητες πληροφορίες όπως τον αριθμό της κάρτας (PAN) αφού έχει ήδη προχωρήσει η εξουσιοδότηση της πληρωμής από τον Issuer ή να αντικαταστήσουν πληροφορίες επιπέδου data-at-rest στους servers του Acquirer ή τις βάσεις του Merchant. Τα Payment Tokens, ήταν μεταγενέστερα μοντέλα τα οποία υποστηρίχθηκαν από τα specifications της EMVCo, σύμφωνα με τα οποία οι TSPs εκδίδουν tokens στους Token requestors (TRs) εκ μέρους των τραπεζών. Τα Payment tokens αντικαταστούν τα PANs και αποθηκεύονται, ανάλογα με την υλοποίηση είτε στο Secure Element ενός κινητού ή σε κάποιο Server από τον οποίο καλούνται όταν χρειαστεί (Host Card Emulation Μοντέλο).

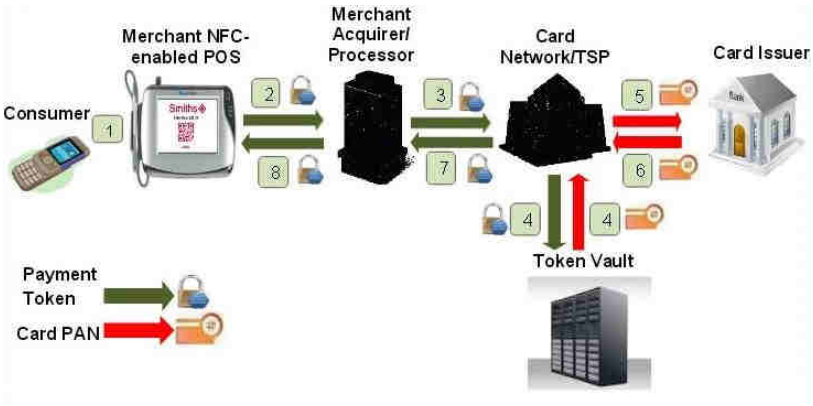
Το σχήμα **(εικόνα_3)**, περιγράφει την ροή του security token μηχανισμού.



Εικόνα 3 Μηχανισμός Acquirer Token, Federal Reserve Banks of Boston & Atlanta

1. Ο πελάτης είναι μπροστά στο POS τερματικό και εκτελεί την πληρωμή.
2. Το τερματικό κρυπτογραφεί τα δεδομένα και τα στέλνει στον Acquirer
3. Αυτός με τη σειρά του προωθεί τα δεδομένα στο Payment (Card) Network και από εκεί στον (card)Issuer για έγκριση
4. Τα δεδομένα μαζί με την έγκριση επιστρέφουν μέσω του Payment Network, στον Acquirer,
5. ο οποίος τα στέλνει στον TSP για να γίνει το Tokenization.
6. Από εκεί επιστρέφουν στον Acquirer, ο οποίος αποθηκεύει το token της συναλλαγής και
7. προωθεί την έγκριση μαζί με το token πίσω στο POS του Merchant.

Το σχήμα (**εικόνα_4**) μας δείχνει το πιο σύγχρονο μοντέλο λειτουργίας με τα Payment Tokens. Το payment token είναι μια τυχαία τιμή η οποία αντικαθιστά τον αριθμό PAN της κάρτας του Cardholder όταν αυτός ξεκινά μία διαδικασία πληρωμής. Από την στιγμή που ο Merchant δεν έχει ποτέ στα χέρια του το PAN, οποιαδήποτε απόπειρα για απάτη θα αποκάλυπτε μόνο το token. Επιπλέον, στην διαδικασία μεταφοράς των πληροφοριών πληρωμής το token δεν μεταφέρεται μόνο του αλλά συνδυάζεται και με ένα **dynamic cryptogram** (ένα μοναδικό κλειδί, ξεχωριστό για κάθε συναλλαγή) το οποίο αποτρέπει τις replay attacks. Η προστασία του PAN σε όλη τη διάρκεια της συναλλαγής είναι η ουσιώδη διαφορά ανάμεσα στα δύο μοντέλα tokenization.



Εικόνα 4 Μηχανισμός Issuer Token, Federal Reserve Banks of Boston & Atlanta

Τα Payment tokens μπορεί να είναι σταθερά, δυναμικά ή συνδυασμός και των δύο. Το μοντέλο EMVCo υποστηρίζει το στατικό μοντέλο για τους εξής λόγους:

1. είναι δύσκολο για μερικούς Issuers να ενσωματώσουν dynamic tokens στις κονσόλες διαχείρισης των κλειδιών τους στα authorization/authentication συστήματα τους.
2. Περιορισμένος αριθμός **Bank Identification Numbers** (BINs, τα 4-6 πρώτα ψηφία σε μια κάρτα τα οποία προσδιορίζουν τον Issuer) για την ανάθεση σε κάθε domain και συσκευή αν όλο το σύστημα είναι dynamic.
3. Οι Merchants θα δυσκολεύονταν να κρατήσουν συνεχή αντιστοίχιση πελάτη/στοιχείων αν άλλαζε το token σε κάθε συναλλαγή.

Σε γενικές γραμμές, το static (BIN) token ευθυγραμμίζεται με την λογική δρομολόγησης του δικτύου της πληρωμής και λύνει τα χέρια των τραπεζών σε θέματα διαχείρισης και αρχιτεκτονικής.

Αναλύοντας λοιπόν τα σχήμα έχουμε τα εξής διακριτά βήματα:

1. Ο cardholder πιστοποιεί μια συναλλαγή στο τερματικό POS.
2. Το POS στέλνει την πληροφορία (**token** + **cryptogram** + **δεδομένα συναλλαγής**) κρυπτογραφημένα προς τον Acquirer.
3. Ο Acquirer προωθεί όλη την παραπάνω πληροφορία στο Payment Network όπου έχει και τον ρόλο του TSP.
4. Επικοινωνεί με το Token Vault, ώστε να κάνει την αντιστοίχιση του token με το PAN.

5. Στέλνει το PAN στον (card) Issuer για έγκριση (ή απόρριψη).
6. Ο Issuer στέλνει την απάντηση του πίσω στο Payment Network και αυτό με τη σειρά του
7. Επιστρέφει το token, πλέον, της κάρτας μαζί με την απάντηση του Issuer στον Acquirer.
8. Τέλος, η τελική πληροφορία, φτάνει στο POS του Merchant για να ολοκληρωθεί η διαδικασία.

Από τα δύο πρότυπα, φαίνεται ότι η παρουσία token σε συνδυασμό με encryption σε όλα (σχεδόν) τα βήματα της συναλλαγής, προσφέρουν την μεγαλύτερη δυνατή ασφάλεια και πάνω σε αυτό το πρότυπο θα στηριχθεί και το μοντέλο των mobile wallets. Η ανάγκη αυτή έγινε σαφής από την εποχή που επικράτησαν οι κάρτες chip-and-pin έναντι των κλασσικών mag-stripe καρτών. Διάφορα μοντέλα δοκιμάστηκαν στην πορεία αλλά το επικρατέστερο ήταν αυτό της EMVCo, με τα σημαντικότερα χαρακτηριστικά του να είναι ο συνδυασμός static token και dynamic cryptogram αλλά κυρίως η συμμετοχή όλων των εμπλεκόμενων μερών μιας συναλλαγής στη ροή του token μέχρι και το de-tokenization μέσω του token vault από τον Issuer. Με την EMVCo συντάχθηκαν και οι υπόλοιποι συνασπισμοί καθώς και Payment Networks όπως οι Visa, Mastercard και American Express (4), για διεξοδικότερη έρευνα και βελτίωση. Η δομή του EMV μοντέλου αναφέρει τους ρόλους και τις κύριες ευθύνες του κάθε ρόλου για την κάθε συμμετέχον οντότητα μέσα στο ecosystem των συναλλαγών. Ως πιο χαρακτηριστικά, ξεχωρίζουν τα παρακάτω:

- Το format του token θα πρέπει να είναι παρόμοιο με αυτό του PAN της κάρτας, δηλαδή, 13-19 ψηφία τα οποία θα πρέπει να επαληθεύονται κατά ISO 8583 σύμφωνα με τα πρότυπα του οργανισμού για τους αριθμούς καρτών (το token δηλαδή, είναι μεν τυχαίο, αλλά όχι χωρίς καμία δομή)
- Θα είναι domain-specific, και θα έχουν αξία μόνο στο συγκεκριμένο domain.
- Το PAN θα πρέπει να είναι γνωστό μόνο στον cardholder και στον Issuer, ενώ οι υπόλοιπες οντότητες θα γνωρίζουν μόνο το token

- Θα πρέπει να γίνεται επιβεβαίωση του **Token Requester** (**TR**) κάθε φορά που γίνεται αίτημα για token

Σε μελλοντικές εκδόσεις του μοντέλου της EMVCo, αναμένεται να γίνουν διασαφηνίσεις, όπως για παράδειγμα ποιες οντότητες θα μπορούσαν να έχουν ρόλο TSP και ποια κριτήρια θα πρέπει να καλύπτουν ή να γίνει πιο συγκεκριμένη η διαδικασία αίτησης token από έναν TR. Αναφέρονται όμως επιγραμματικά, οι πιο βασικές οντότητες μαζί με τις ιδιότητες τους, όπως συναντώνται τώρα,

- **Token Service Provider (TSP)**, αναλαμβάνουν την δημιουργία και διανομή των tokens στους ενδιαφερόμενους, τον έλεγχο των ενδιαφερόμενων φορέων (TRs), ελέγχουν τον κύκλο ζωής τους, την ασφάλεια και τους ελεγκτικούς μηχανισμούς που το προστατεύουν, και εντοπίζουν τα domains στα οποία έχουν ισχύ τα tokens και τι κανόνες τα χαρακτηρίζουν. Διάφορες οντότητες μπορούν να έχουν τον ρόλο ενός TSP όπως Issuers, Acquirers, Payment Networks, ακόμα και Merchants. Δεν υπάρχουν άμεσα σαφή κριτήρια για να γίνει κάποιος TSP αλλά δεν υπάρχουν και ξεκάθαρες απαγορευτικές γραμμές. Συμφέρει πάντως, ως έχει, να έχουν TSP ρόλο τα Payment Networks, καθαρά και μόνο λόγω εμπειρίας και δομής σε θέματα διανομής και επεξεργασίας ευαίσθητης πληροφορίας, αλλά και θέσης του στην διαδικασία μιας συναλλαγής.

- **Token Requestor (TR)**, είναι οι οντότητες οι οποίες αιτούνται tokens από τους TSPs με σκοπό να ξεκινήσουν ή ολοκληρώσουν μία συναλλαγή. Μπορεί να είναι εταιρίες παροχής υπηρεσιών mobile wallet, εφαρμογές online αγορών, Issuers, Acquirers, merchants κα. Για να μπορεί να αιτηθεί token μια TR οντότητα οφείλει να κάνει εγγραφή στον TSP αφού πρώτα αποδεχθεί τους όρους χρήσης και συμμόρφωσης. Μετά την εγγραφή λαμβάνει ένα TR Id και το αντίστοιχο API ώστε να ενσωματώσει στα συστήματα του και να επικοινωνεί με τον TSP. Οπότε πλέον, ο TR θα μπορεί να κάνει αιτήσεις για tokens από τον TSP για να το προωθεί στα Secure Elements των NFC-enabled συσκευών (θα γίνει αναφορά σε αυτά παρακάτω) των cardholders.

- **Payment Network,** ως TSPs πέρα από τους συνήθεις ρόλους τους, αναλαμβάνουν και την εγκατάσταση και διανομή των TRs APIs, την δημιουργία των δικών τους Token Vaults, της πλατφόρμας για την διανομή των tokens και των token registries (5)
- **Merchant,** πέρα από τον συνήθη ρόλο τους, μπορούν να αιτηθούν token ως TRs για τις περιπτώσεις πχ που έχουμε card-on-file (κρατάει στοιχεία για να είναι πιο γρήγορες οι μελλοντικές συναλλαγές). Εάν αποκτήσει τέτοιο ρόλο, οφείλει να ενσωματώσει το API του TSP στο σύστημα του για να μπορεί να αιτηθεί tokens.

2. Τεχνολογίες που σχετίζονται με τα Mobile Wallets

2.1. Τυπικό Πορτοφόλι

Πριν γίνει η αποκρυπτογράφηση ενός ψηφιακού πορτοφολιού, ας γίνει μία γρήγορη αναφορά στο πως είναι ένα πραγματικό πορτοφόλι. Το κλασσικό (συνήθως δερμάτινο) πορτοφόλι έχει στα περιεχόμενα του μετρητά, κάρτες συναλλαγών (debit, πιστωτικές), κάρτες που πιστοποιούν ταυτότητα ή ικανότητα του κατόχου (ταυτότητα, δίπλωμα οδήγησες, διαβατήριο κτλ.) κάρτες μέλους (καταστήματα, clubs, βιβλιοθήκες), αποδείξεις (αγορές, πληρωμές, ATM) ακόμα και διάφορες σημειώσεις (ραντεβού, ψώνια, τηλέφωνα, διευθύνσεις, ονόματα, to do lists κτλ.). Όπως αναφέρθηκε και στην εισαγωγή, στο πλαίσιο αυτής της εργασίας δεν παρουσιάζεται κάποια ψηφιακή λύση τόσο ολοκληρωμένη ώστε να είναι εφικτό να γίνεται άμεσα κουβέντα για την πλήρη αντικατάσταση του. Η πλειοψηφία των λύσεων που κυκλοφορούν στοχεύουν στην εκμετάλλευση των τραπεζικών (και όχι μόνο, gift κάρτες, loyalty κάρτες) καρτών. Μόλις όμως λυθεί το ζήτημα αποθήκευσης και αναγνώρισης ως αποδεικτικού στοιχείου, μέσα από κινητό τηλέφωνο, κρατικών εγγράφων (για παράδειγμα ταυτότητα & δίπλωμα οδήγησης) τότε το τυπικό πορτοφόλι θα πλησιάζει προς την κατάργηση του.

2.2. Πως Λειτουργεί μία τυπική κάρτα Mag Stripe

Πάνω στην μπροστινή μεριά της κάρτας υπάρχει ο αριθμός της κάρτας CCN(credit card number), ο οποίος είναι μία αλληλουχία 12-20 ψηφίων του δυαδικού συστήματος(**εικόνα_5**). Το σύνηθες είναι τα 16 ψηφία (6). Τα πρώτα 6 ψηφία είναι το IIN (issuer identification number, στην βιβλιογραφία αναφέρεται και ως BIN, Bank Identification Number), τα οποία και προσδιορίζουν το σύστημα που χρησιμοποιείται (Visa, Mastercard κτλ.), την Issuer τράπεζα, και/ή το νόμισμα που χρησιμοποιείται. Τα επόμενα 7-15 ψηφία (το λεγόμενο PAN) προσδιορίζουν τον λογαριασμό με τον οποίο είναι συνδεμένη η κάρτα. Το τελευταίο ψηφίο είναι και το πιο σημαντικό καθώς αποτελεί το λεγόμενο checksum, είναι δηλαδή ένα hash όλων των προηγούμενων ψηφίων της κάρτας και σκοπός του είναι να πιστοποιεί την γνησιότητα της κάρτας κατά τις συναλλαγές αλλά και να προφυλάσσει από λάθη (πχ, εάν περαστεί λάθος ο αριθμός της κάρτας σε ένα τερματικό πληρωμών).

Εικόνα 5 Επεξήγηση Αριθμού Κάρτας, Broken Secrets

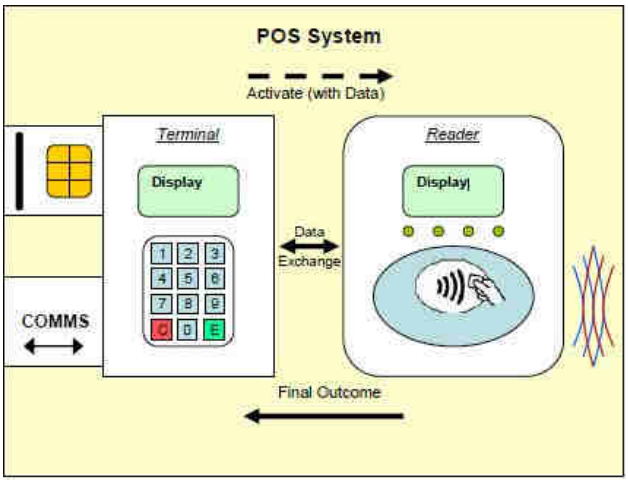
Τα δεδομένα της κάρτας εγγράφονται πάνω στην μαγνητική ταινία η οποία είναι χωρισμένη σε τρία “tracks”. Στο 1ο track καταγράφεται το πλήρες νούμερο της κάρτας (CCN), το όνομα του κατόχου της κάρτας, η ημερομηνία λήξης. Στο 2ο track υπάρχουν τα παραπάνω δεδομένα και επιπλέον ο αριθμός CVV1, ο οποίος έχει την ίδια λειτουργία με το κλασσικό CVV2 που βρίσκεται στο πίσω μέρος της κάρτας, απλά σε αντίθεση με τον CVV2 ο οποίος παρέχει verification για τις “Card not Present” (CnP) συναλλαγές (δηλαδή τις online αγορές όπου η κάρτα δεν είναι παρών), ο CVV1 χρησιμοποιείται για τις συναλλαγές σε φυσικό κατάστημα μπροστά σε κάποιο τερματικό. Τέλος, στο 3ο track υπάρχει πάλι το πλήρες νούμερο της κάρτας μαζί με κάποια επιπλέον δεδομένα και κωδικούς ασφάλειας .

Σε μία συναλλαγή “Card Present”, η διαδικασία πληρωμής ξεκινάει με την υποβολή του αριθμού της κάρτας είτε με πληκτρολογώντας τον αριθμό είτε περνώντας την κάρτα μέσα από ένα MSR. Στην πλειοψηφία των συναλλαγών, ο CCN περνάει απευθείας, μέσω του Merchant, στον Acquirer, την τράπεζα δηλαδή με την οποία ο Merchant συνεργάζεται. Συνήθως, η διαδικασία περιλαμβάνει και την επιβεβαίωση τόσο του Payment Network (Visa, Mastercard κτλ.) όσο και Issuer.

2.3. Λειτουργία Τυπικού Συστήματος POS

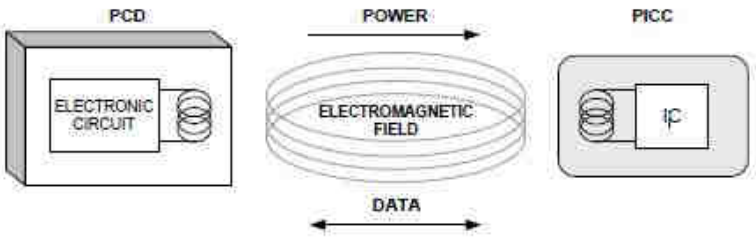
Σύμφωνα με το μοντέλο της EMVCo (5)**,** ένα τυπικό σύστημα POS, περιγράφεται στο σχήμα **(εικόνα_6)**, όπου στην δεξιά μεριά φαίνεται το κομμάτι που αντιπροσωπεύει τον αναγνώστη ο οποίος επικοινωνεί με την κάρτα EMV και παρέχει την εφαρμογή για την ανέπαφη επικοινωνία. Είναι δηλαδή το σημείο εισόδου της πληροφορίας. Επίσης, παρέχει το User Interface, την οθόνη δηλαδή όπου ο κάτοχος της κάρτας βλέπει τα στοιχεία, και πιθανόν διάφορα display leds. Στην αριστερή μεριά παρατηρούμε μια συμβολική εικόνα του τμήματος του POS που βλέπει ο Merchant, όπου περιλαμβάνει μία μέθοδο εισαγωγής δεδομένων(συνήθως

πληκτρολόγιο) μία οθόνη, το Interface για την online επικοινωνία αλλά και Interfaces για κάρτα μαγνητική ή επαφής.



Εικόνα 6 Αρχιτεκτονική ενός POS, EMV-Contactless Specifications for Payment System

Στο σχήμα **(εικόνα_7)**, φαίνεται πως γίνεται η επικοινωνία σε ηλεκτρονικό επίπεδο μεταξύ μιας EMV κάρτας και ενός POS τερματικού. Τα βασικά στοιχεία του είναι ο ανέπαφος αναγνώστης PCD (proximity coupling device) και η EMV κάρτα, ή PICC (proximity IC card). Ο PCD είναι μια κεραία συνδεμένη σε ένα ηλεκτρονικό κύκλωμα. Η PICC αποτελείται από μία επαγωγική κεραία και ένα ηλεκτρονικό κύκλωμα ενσωματωμένο σε αυτήν. Ο συνδυασμός PCD και PICC συμπεριφέρεται ως ένας μετασχηματιστής. Ένα εναλλασσόμενο ρεύμα περνάει μέσα από το κυρίως πηνίο (κεραία PCD) και δημιουργεί ένα ηλεκτρομαγνητικό πεδίο, το οποίο παρέχει ρεύμα στο δευτερεύον πηνίο της PICC. Το PICC μετατρέπει το ρεύμα αυτό σε DC τάση και παρέχει έτσι ρεύμα στο ηλεκτρονικό κύκλωμα πάνω στο πηνίο της κάρτας.



Εικόνα 7 Επικοινωνία EMV Κάρτας & POS, EMV-Contactless Specifications

Το σημαντικό όμως κομμάτι είναι η προσθήκη πληροφορίας επάνω στο ηλεκτρονικό ή οπτικό σήμα. Αυτό επιτυγχάνεται με συνδυασμό διαφόρων μεθόδων διαμόρφωσης, για την ακρίβεια διαμόρφωσης πλάτους του σήματος (πόσο σήμα μεταφέρεται ανά μονάδα χρόνου) και

διαμόρφωση φάσης, κατά πόσο δηλαδή θα υπάρχει προώθηση ή καθυστέρηση στη ροή του σήματος που μεταφέρεται. Οπότε, η RF ενέργεια που μεταφέρεται, δεν ενεργοποιεί απλά την κάρτα αλλά μεταφέρει και δεδομένα από το POS. Η κάρτα επεξεργάζεται τα δεδομένα και απαντά στο PCD με μέθοδο διαμόρφωσης φορτίου η οποία στηρίζεται σε ηλεκτρομαγνητική σύζευξη μεταξύ PCD και PICC, όπου το PICC αλλάζει την τιμή του ρεύματος στην κεραία, κάτι που το αντιλαμβάνεται το PCD από την δική του κεραία.

2.4. Λειτουργία Τυπικής Κάρτας EMV

EMV είναι τα αρχικά των Europay, Mastercard και Visa, οι τρεις πρώτοι οργανισμοί οι οποίοι ανέπτυξαν τα αρχικά χαρακτηριστικά και specifications για τις chip κάρτες. Αργότερα προστέθηκαν και άλλοι οργανισμοί και ο σκοπός ήταν να υπάρχει διαλειτουργικότητα ανάμεσα στις συναλλαγές βάση κάρτας ανεξαρτήτους παρόχου και οικονομικού οργανισμού. Ο οργανισμός σήμερα λέγεται EMVCo. Οι EMV κάρτες, έχοντας χαρακτηριστικά όπως **Κρυπτογράφηση** (περιλαμβάνοντας end-to-end κρυπτογραφία (E2EE) ή point-to-point κρυπτογραφία (P2PE), με την οποία απευθείας κρυπτογραφεί τα δεδομένα που εισέρχονται σε ένα τερματικό ενός Merchant με επίδειξη της κάρτας (swipe, entry, tap) και **Tokenization (**με το οποίο τα δεδομένα της κάρτας θα αντικαθίστανται με ένα άλλο, μίας χρήσης value, ώστε ακόμα και εάν γίνει υποκλοπή, να μην μπορεί να χρησιμοποιηθεί πουθενά), ενισχύουν την συναλλαγή μέσω κάρτας στις εξής τρεις περιοχές: αυθεντικοποίηση της κάρτας, πιστοποίηση του χρήστη και εξουσιοδότηση της πληρωμής.

Πιο συγκεκριμένα, στο κομμάτι της **αυθεντικοποίησης της κάρτας**, οι συναλλαγές για να προχωρήσουν, χρησιμοποιούν τρεις μεθόδους (5): 1. SDA (static data authentication), 2. DDA (dynamic data authentication) και 3. CDA (combined DDA). Οι διαφορές τους γίνονται σαφής μόλις δούμε κάποια επιπλέον χαρακτηριστικά στην λειτουργία των καρτών.

Οι κάρτες αυτές λειτουργούν με εφαρμογές, συνήθως κάθε κάρτα έχει μία εφαρμογή η οποία έχει να κάνει με την εταιρία που την υποστηρίζει (πχ VISA εφαρμογή), αν και θεωρητικά τα specs των καρτών υποστηρίζουν και περισσότερες από μια εφαρμογές. Τα δεδομένα που έχουν μέσα οι εφαρμογές αυτές είναι μη μεταβλητά(fixed) και έχουν υπογραφεί ψηφιακά από το κλειδί της εκδότριας αρχής. Το κλειδί αυτό έχει certification το οποίο έχει εκδοθεί από την CA που συνεργάζεται με το Payment Network πίσω από την κάρτα (πχ VISA, Mastercard). Κατά την επικοινωνία κάρτας με τερματικό POS η κάρτα στέλνει το παραπάνω certificate από τον

issuer όπως και την υπογραφή (των πάγιων δεδομένων). Το POS έχει τα public κλειδιά των CA και έτσι μπορεί να πιστοποιήσει την γνησιότητα της κάρτας. Αυτό το σενάριο περιγράφει την SDA μέθοδο.

Στις μεθόδους DDA και CDA, η κάρτα έχει το δικό της ζεύγος κλειδιών, οπότε η επικοινωνία πλέον είναι δυναμική καθώς δεν ζητάει να γίνει ταυτοποίηση μιας ψηφιακής υπογραφής τμημάτων πληροφορίας που υπήρχαν στην κάρτα. Τα δεδομένα που ζητούνται για υπογραφή περιλαμβάνουν και ένα τυχαίο νούμερο το οποίο παρέχεται από το POS.

Οι αλγόριθμοι που χρησιμοποιούνται στα παραπάνω(CA κλειδιά, πιστοποιητικά, υπογραφές) είναι RSA και SHA-1.

Στο κομμάτι της **πιστοποίησης του κατόχου** της κάρτας (CVM), συναντούμε 4 μεθόδους,

- Offline PIN, με την πληροφορία κρυπτογραφημένη ή σε plaintext μορφή
- Online PIN, με την πληροφορία να στέλνετε στην issuer αρχή για επιβεβαίωση, αφού πρώτα κρυπτογραφηθεί στο pin pad
- Υπογραφή, (ισχύει ακόμα στην Αμερική)
- Καθόλου πιστοποίηση

Στο σενάριο της offline PIN μεθόδου ταυτοποίησης του κατόχου (με κρυπτογράφηση), η κάρτα στέλνει το PIN κρυπτογραφημένο από το δικό της ζεύγος κλειδιών, μαζί με ένα τυχαίο κρυπτογράφημα για την αποφυγή replay attacks, στο τερματικό POS. Το POS διαβάζει το PIN και αφού το κρυπτογραφεί με το public κλειδί της κάρτας, της το επιστρέφει για να ολοκληρωθεί η επικοινωνία (handshake)

Τέλος, αναφορικά με την τελική **εξουσιοδότηση της πληρωμής**, γίνεται είτε online είτε offline. Στο Online σενάριο (7)**,** η πληροφορία στέλνεται στον Issuer (μαζί με ένα One-time κρυπτογράφημα που αφορά την συναλλαγή και μόνο) για την έγκριση ή απόρριψη της συναλλαγής. Το κρυπτογράφημα αυτό προκύπτει συμμετρικό κλειδί της κάρτας και ονομάζεται ARQC (authorization request cryptogram), ενώ η απάντηση που έρχεται από τον Issuer (εάν υπάρχει έγκριση) λέγεται ARPC (authorization response cryptogram).

Στο offline σενάριο, η επικοινωνία περιορίζεται στην EMV κάρτα και το τερματικό, χρησιμοποιείται ασύμμετρη κρυπτογραφία και η κάρτα αποφασίζει (βάση παραμέτρων ρίσκου που έχει ορίσει ο Issuer) αν θα προχωρήσει η συναλλαγή. Τέτοιες παράμετροι μπορεί να είναι, α. εάν έχει περάσει ένα ποσό συναλλαγών, οπότε κάνει prompt για online έλεγχο,

β. εάν έχει γίνει μεγάλος αριθμός συνεχόμενων offline συναλλαγών, οπού και πάλι μπορεί να κριθεί απαραίτητο να γίνει online έλεγχος.

2.5. Λειτουργία NFC

NFC είναι τα αρχικά για το Near Field Communication και όπως μαρτυρά και το όνομα, είναι μια τεχνολογία ασύρματης επικοινωνίας κοντινής απόστασης, συνήθως μικρότερης των 5cm. Το NFC επιτρέπει την ανταλλαγή μικρών πακέτων πληροφοριών (payloads) μεταξύ 2 συσκευών ή μιας συσκευής και ενός NFC Tag (η ίδια αρχή παρατηρείται και στις κάρτες EMV). Υπάρχουν 4 τύποι NFC Tags (8), και οι διαφορές τους βρίσκονται στην χωρητικότητα και την ταχύτητα μεταφοράς των δεδομένων.

- **Type 1** tags συνήθως φτάνουν τα 96 bytes χωρητικότητα με ταχύτητα 106Kbps (kilobits per sec),
- **Type2** είναι από 48 μέχρι 2KB πληροφορία και ταχύτητες στα106Kbps,
- **Type3** στα 2KB δεδομένα και ταχύτητες στα 212Kbps, ενώ τα
- **Type4** φτάνουν μέχρι και τα 32KB και ταχύτητα τα 424Kbps.

Η βασική αρχιτεκτονική των NFC Tags, είναι σαν αυτή των RFID, αλλά με μερικές διαφορές. Είναι παθητικά, δεν έχουν δηλαδή δική τους τροφοδοσία αλλά ενεργοποιούνται από την συσκευή που πάει να τα διαβάσει μέσω μαγνητικής επαγωγής. Όσο πιο μεγάλη η μνήμη συνήθως τόσο αυξάνει και το μέγεθος του Tag.

Οι NFC συσκευές υποστηρίζουν στο σύνολο τους τρεις τρόπους λειτουργίας (9)**,**

1. Reader/writer mode, όπου μια συσκευή με NFC δυνατότητα μπορεί να διαβάσει ή/και να γράψει NFC Tags και αυτοκόλλητα.
2. P2P mode (peer to peer), όπου 2 NFC συσκευές ανταλλάσσουν δεδομένα μεταξύ τους
3. Card emulation mode, όπου η NFC συσκευή λειτουργεί και εξομοιώνει μια NFC κάρτα. Σε αυτή την μορφή, η συσκευή μπορεί να επικοινωνήσει και να διαβαστεί από μια εξωτερική συσκευή ανάγνωσης NFC, όπως για παράδειγμα ένα NFC τερματικό POS.

Τα μηνύματα που μεταφέρονται είναι τεχνολογίας **Ndef**(περισσότερα για αυτό παρακάτω) και μπορεί να είναι τύπου,

- Smart Poster, για ανάγνωση επιπλέον πληροφορίας από διαφημιστικά posters
- Handover, για την άμεση σύνδεση δύο συσκευών με το άγγιγμα τους
- vCard, για την μεταφορά δεδομένων υπό μορφή vCard
- URL, για να έχω απευθείας σύνδεση με ιστοσελίδα.

Το Ndef (NFC Data Exchange Format) είναι ένα ελαφρύ binary μήνυμα σχεδιασμένο να ενθυλακώνει (encapsulate) ένα ή περισσότερα σαφώς ορισμένα από εφαρμογή τμήματα πληροφορίας (payloads) σε ένα ενιαίο format μηνύματος και να αποστέλλεται ενιαίο. Το κάθε Ndef μήνυμα περιέχει Ndef records (10)**,** το κάθε ένα από τα οποία περιέχει από ένα payload πληροφορίας με μέγεθος που φτάνει τα 2^{32}-1 bytes. Τα records συνδέονται μεταξύ τους δημιουργώντας αντίστοιχα μεγαλύτερα payloads. Το κάθε Ndef record, χρησιμοποιεί τρεις παραμέτρους για να περιγράψει το κάθε payload που μεταφέρει:

- Μήκος Payload, για να περιγράψει πόσα Bytes πληροφορίας υπάρχει στο payload.
- Είδος Payload, καθώς υποστηρίζει URLs, NFC-specific είδους format και MIME media, επιπλέον από ότι αναφέρθηκε παραπάνω.
- Αναγνωριστικό (identifier) του Payload, στην μορφή ενός URL ώστε να κάνει διασταύρωση σε άλλα payloads (όταν υποστηρίζεται URL Linking)

Επιγραμματικά λειτουργεί ως εξής, έστω ότι υπάρχει ένα μήνυμα το οποίο πρέπει να μεταφερθεί μέσω NFC από συγκεκριμένη εφαρμογή(πχ στην επικοινωνία κινητού σε Card emulation mode με ένα NFC POS). Η γεννήτρια Ndef σπάει το μήνυμα σε payloads και τα ενθυλακώνει σε Ndef records, αποσαφηνίζοντας τον τύπο και το μήκος του κάθε payload (ίσως και ενός identifier). Τα Ndef records συνδέονται ώστε να σχηματιστεί ένα ενιαίο Ndef μήνυμα. Το μήνυμα αυτό παραδίδεται ολόκληρο (ποτέ σε κομμάτια) στην συσκευή-δέκτη NFC (ή μπορεί να υπάρχει ενδιάμεσα ένα NFC Tag) όπου και διαχωρίζεται στα δομικά του payloads. Για να ξεχωρίσω την αρχή και το τέλος του μηνύματος, η αρχή μαρκάρεται με ένα MB (message begins) και το τέλος με ένα ME (message ends). Υπάρχει δε η δυνατότητα να μεταφερθεί ένα ολόκληρο Ndef μήνυμα ως payload ενός Ndef record.

Ο πρόγονος του NFC ήταν το RFID, το οποίο εμφανίστηκε κοντά στο 1980. Όταν άρχισε να παίρνει μορφή, έγινε πολύ μεγάλη προσπάθεια, ώστε να δημιουργηθούν αυστηρά πρότυπα για την λειτουργία του NFC, όπως το ISO/IEC 14443 (11) καθώς φαίνεται ως το πιο ελπιδοφόρο πρότυπο στις ασύρματες επικοινωνίες μικρής απόστασης. Οι πιο σημαντικές έγιναν από την GSMA(GSM Association) αλλά και το NFC Forum ιδρυτικά μέλη του οποίου ήταν οι SONY, Nokia και NXP Semiconductors (το 2013 είχε φτάσει τα 180 μέλη). Το 2006 άρχισε να εμφανίζεται σε διάφορες εφαρμογές και έγινε και η εμφάνιση του πρώτου τηλεφώνου (Nokia 6131) με πρώιμη τεχνολογία NFC ικανό να διαβάζει NFC tags. Τα tags αυτά χρησιμοποιήθηκαν σε καταστήματα, λεωφορεία και διάφορα σημεία πληρωμών. Τέλος το 2009 έγινε δυνατή και η P2P χρήση όπου οδηγεί τις εξελίξεις σε συνδυασμό με την προώθηση των πληρωμών μέσω mobile wallet.

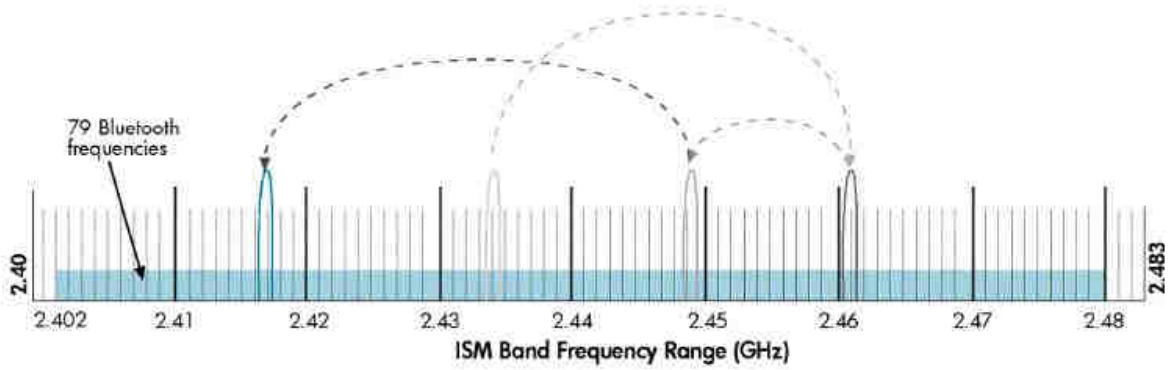
2.6. Λειτουργία Bluetooth και Bluetooth Low Energy

Το Bluetooth είναι ένα standard δικτύωσης που χρησιμοποιείται για μικρής κλίμακας δίκτυα. Το όνομα του, προέρχεται από έναν Βασιλιά της Δανίας του 10^{ου} αιώνα του οποίου το ψευδώνυμο ήταν “Μπλε Δόντι” και το σχήμα που έχει το σύμβολο του Bluetooth, είναι ο συνδυασμός των 2 Σκανδιναβικών ρουνικών που μεταφράζονταν ως το όνομα του βασιλιά.

Σαν standard δουλεύει σε 2 επίπεδα, σε ένα φυσικό επίπεδο μεταξύ συσκευών, και σε ένα επίπεδο πρωτοκόλλου, όπου οι δύο συσκευές θα πρέπει να συμφωνήσουν ως προς το πότε θα στέλνεται πληροφορία, πόση πληροφορία κάθε φορά και πως οι συσκευές θα ξέρουν ότι η πληροφορία που στάλθηκε είναι αυτή που παραλήφθηκε και vice-versa.

Ξεκινώντας από τα βασικά, το Bluetooth μπορεί να συνδέσει μέχρι και 8 συσκευές ταυτόχρονα. Οι συσκευές μπορούν να έχουν μία μέγιστη απόσταση των 10 μέτρων, λόγω χαμηλής κατανάλωσης. Παρόλα αυτά, δεν χρειάζεται οι συσκευές να έχουν οπτική επαφή μεταξύ τους και δεν διακόπτεται η επικοινωνία από τοίχους. Επίσης, παρότι οι συσκευές είναι κοντά μεταξύ τους, η επικοινωνία τους δεν διακόπτεται χάριν της τεχνολογίας που ονομάζεται **spread-spectrum frequency hoping** (12), σύμφωνα με την οποία η συσκευή θα χρησιμοποιεί κάθε φορά μια συχνότητα από ένα πλήθος 79 διαφορετικών, οι οποίες έχουν επιλεχθεί για την συγκεκριμένη συσκευή από συγκεκριμένο εύρος συχνοτήτων. Από την στιγμή που οι

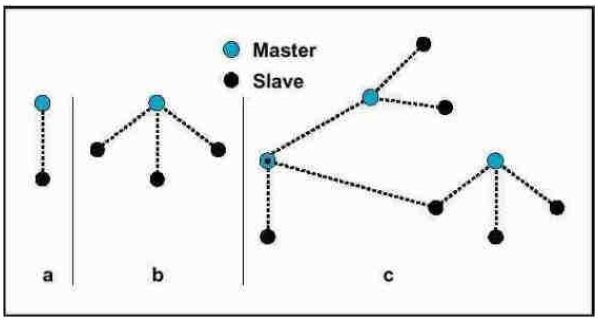
αναμεταδότες στα Bluetooth αλλάζουν συχνότητες 1600 φορές το δευτερόλεπτο **(εικόνα_8),** είναι πού δύσκολο δύο συσκευές Bluetooth να είναι ταυτόχρονα στην ίδια συχνότητα.



Εικόνα 8 Αλλαγές Συχνότητας στο Bluetooth, HP-Bluetooth Wireless Technology Basics

Συγκεκριμένα για τις BLE υλοποιήσεις, το **ISM band** χωρίζεται σε 40 κανάλια 2 ειδών, τα κανάλια Advertising και τα κανάλια Δεδομένων. Τα Advertising κανάλια, τρία στο σύνολο, χρησιμοποιούνται για την ανακάλυψη συσκευών, την έναρξη της μεταξύ τους επικοινωνίας και εκπομπής δεδομένων. Τα κανάλια Δεδομένων, 37 στο σύνολο, χρησιμεύουν στην ανταλλαγή δεδομένων μεταξύ των Bluetooth συσκευών μόλις έχει γίνει η μεταξύ τους σύνδεση.

Όταν λοιπόν δύο ή περισσότερες συσκευές Bluetooth βρίσκονται στον ίδιο χώρο, μία ηλεκτρονική επικοινωνία ξεκινά μεταξύ τους αυτόματα, χωρίς να χρειαστεί να πατηθεί κάποιο πλήκτρο. Μόλις ολοκληρωθεί η επικοινωνία σχηματίζεται ένα μικρό, προσωπικό δίκτυο PAN (personal area network) γνωστό και ως **piconet**. Μόλις αυτό εδραιωθεί, οι συσκευές αλλάζουν συχνότητα συντονισμένα χρησιμοποιώντας το ίδιο κανάλι, αποφεύγοντας άλλα αντίστοιχα δίκτυα μέσα στον ίδιο χώρο. Στο **(εικόνα_9)** παρουσιάζονται τρεις χαρακτηριστικές τοπολογίες ενός και περισσότερων piconets. Στο a, είναι η πιο απλή του μορφή με 2 συσκευές συνδεμένες, στο b, παρουσιάζεται ένα piconet με 4 συσκευές ενώ στο c, απεικονίζεται ένα συνδυασμό από τρία piconets (ή **Scatternet**, όταν είναι πάνω από ένα).

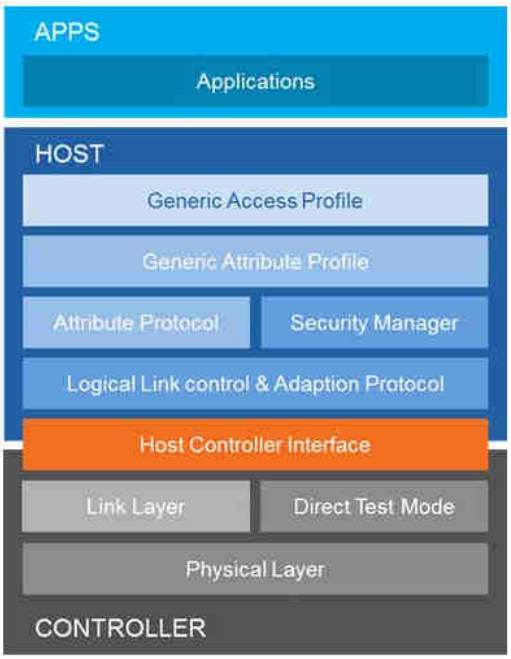


Εικόνα 9 Τοπολογίες Piconets, Bluetooth by Inigo Puy, 05/05/2008

Πιο συγκεκριμένα, οι δύο επικρατέστερες υλοποιήσεις του Bluetooth ήταν η BR/EDR (Bluetooth Basic Rate/Enhanced Data Rate) η οποία είναι γνωστή ως έκδοση 2.0/2.1 και η BLE (Bluetooth Low Energy) έκδοση η οποία είναι γνωστή και ως 4.0/4.1/4.2. Η κάθε υλοποίηση έχει διαφορετικό chipset, αν και έχουν υπάρξει και dual-mode chipsets ανάλογα το σενάριο και σκοπό της υλοποίησης. Οι βασικές διαφορές είναι οι εξής (13)**:**

- BR/EDR, ιδανικό για συνδέσεις κοντινής απόστασης και συνεχής ροής πληροφορίας, ιδανικό για streaming ήχου.
- BLE, ιδανικό για συνδέσεις μεγαλύτερης απόστασης πολύ μικρής διάρκειας (burst), ιδανικό για εφαρμογές όπου απαιτείται μεγάλη διάρκεια ζωής μπαταρίας.
- Dual Mode, ιδανικό για συσκευές όπως μοντέρνα κινητά τηλέφωνα όπου θέλουμε σύνδεση και με BR/EDR συσκευές (πχ ακουστικά) και με BLE συσκευές όπως tags καταστημάτων.

Η αρχιτεκτονική του περιλαμβάνει τέσσερα πρωτόκολλα, RF (radio), LC (link control), LM (Link Manager) και το L2CAP (Logical Link Control and Adaption). Στο **(εικόνα_10)** φαίνονται όλα τα Layers του συστήματος. Ως Bluetooth controller ονομάζονται τα χαμηλότερα τρία επίπεδα, το radio, Link control και το link manager. Αυτή η υλοποίηση είναι αρκετά κοινή καθώς χρησιμοποιεί ένα interface που λέγεται HCI (Host to Controller Interface) το οποίο παρέχει επικοινωνία με το υπόλοιπο σύστημα το Bluetooth Host.



Εικόνα 10 Bluetooth Layers, www.bluetooth.com, Core Specification

Ακολουθεί μία σύντομη περιγραφή του κάθε τμήματος που εμφανίζεται στο σχήμα. Το **PHY** (Physical) layer, το οποίο ελέγχει την μετάδοση αλλά και την παραλαβή του σήματος των 2.4 Ghz μέσα από τα κανάλια επικοινωνίας. Το BR/EDR παρέχει περισσότερα κανάλια με πιο περιορισμένο εύρος (bandwidth), ενώ αντίθετα το BLE έχει λιγότερα κανάλια αλλά μεγαλύτερο εύρος. Το **Link** layer καθορίζει την δομή των πακέτων επικοινωνίας στα κανάλια, αναλαμβάνει την ανακάλυψη και υλοποίηση των συνδέσεων και την αποστολή και λήψη των πακέτων.

Για την υλοποίηση του **BLE**, ανάλογα με το status της συσκευής, ξεχωρίζουν πέντε καταστάσεις του Link Layer στις οποίες μπορεί να βρεθεί (14)**,**

- **Standby**, σε αυτή την κατάσταση δεν μεταδίδει ούτε λαμβάνει πακέτα. Μπορεί να μπει σε αυτή την κατάσταση από οποιαδήποτε άλλη.
- **Advertising**, εδώ μεταδίδει δεδομένα από τα 3 advertising κανάλια που αναφέρθηκαν παραπάνω, και είναι σε ετοιμότητα για τυχόν ανταποκρίσεις από άλλες συσκευές στα δικά του πακέτα. Σε αυτή την κατάσταση μπαίνει από την Standby
- **Scanning**, εδώ ανιχνεύει για πακέτα που έρχονται από τα advertising κανάλια άλλων Bluetooth συσκευών. Και πάλι αυτή η κατάσταση λειτουργίας μπορεί να μπει από την Standby.

- **Initiating**, σε αυτή τη κατάσταση, το Link Layer ακούει το advertising από συγκεκριμένες συσκευές και ετοιμάζεται για σύνδεση με μία από αυτές. Σε αυτή την κατάσταση μπαίνει πάλι μόνο από την Standby.
- **Connection**, εδώ πλέον οι συσκευές έχουν πλέον συνδεθεί μεταξύ τους. Σε αυτή την κατάσταση η συσκευή μπορεί να έχει δύο διακριτούς ρόλους, ανάλογα με την προηγούμενη κατάσταση της συσκευής προτού συνδεθεί,
    - ❖ Master, εάν η συσκευή μπήκε σε Connection mode από Initiating mode
    - ❖ Slave, εάν η συσκευή μπήκε σε Connection mode από Advertising mode

  Ανάμεσα στις δύο συσκευές, αυτή με τον ρόλο Master, θα καθορίζει τους χρονισμούς για την μεταφορά των δεδομένων, ενώ κάθε συσκευή σε Slave ρόλο δεν μπορεί να επικοινωνήσει με παραπάνω από μία συσκευές Master.

Το **Direct Test** mode, επιτρέπει να λάβει εντολή το PHY από testers ώστε να στείλει ή να παραλάβει πακέτα συγκεκριμένης δομής και συχνότητας , μέσω του HCI ή ενός UART interface 2 καλωδίων συνδεμένου σειριακά στην συσκευή (παρέχοντας RS-232C).

Το **HCI** είναι ο συνδετικός κρίκος ανάμεσα στον Bluetooth Controller και το Bluetooth Host.

Το **L2CAP** είναι ένα packet based πρωτόκολλο το οποίο μεταδίδει πακέτα στο HCI ή απευθείας στο Link Manager σε hostless περιβάλλον. Υποστηρίζει multiplexing, διατμηματισμό και επανασύνδεση πακέτων και παροχή πληροφοριών αναφορικά με την ποιότητα άλλων τμημάτων στα υψηλότερα layers. Το **ATT** σε συνδυασμό με GATT (generic attribute profile), είναι αυτό που μόλις πραγματοποιηθεί η επικοινωνία των συσκευών καθορίζει τον τρόπο με τον οποίο θα ανταλλάσσουν δεδομένα και θα μιλάνε μεταξύ τους. Εφαρμόζεται και στα BR/EDR όσο και στα BLE. Ο **Security Manager**, καθορίζει την συμπεριφορά και τα πρωτόκολλα που διαχειρίζονται την σταθερότητα, την κρυπτογράφηση και την αυθεντικοποίηση της σύζευξης των Bluetooth συσκευών, και παρέχει και τα εργαλεία για όλες τις εφαρμογές σε θέματα υποστήριξης ασφάλειας. Το **GATT** (15) που αναφέρθηκε παραπάνω, είναι η υπηρεσία η οποία χωρίζει σε groups τμήματα Bluetooth συσκευών ανάλογα με τα χαρακτηριστικά και τον ρόλο τους ελέγχοντας attributes όπως τρόπο ανάγνωσης και εγγραφής πληροφορίας, τρόπο ειδοποίησης και επικοινωνίας. Χρησιμοποιείται μόνο σε υλοποιήσεις BLE. Τέλος, το **GAP** (generic access profile) δουλεύει συνδυαστικά με το GATT σε υλοποιήσεις BLE και καθορίζει

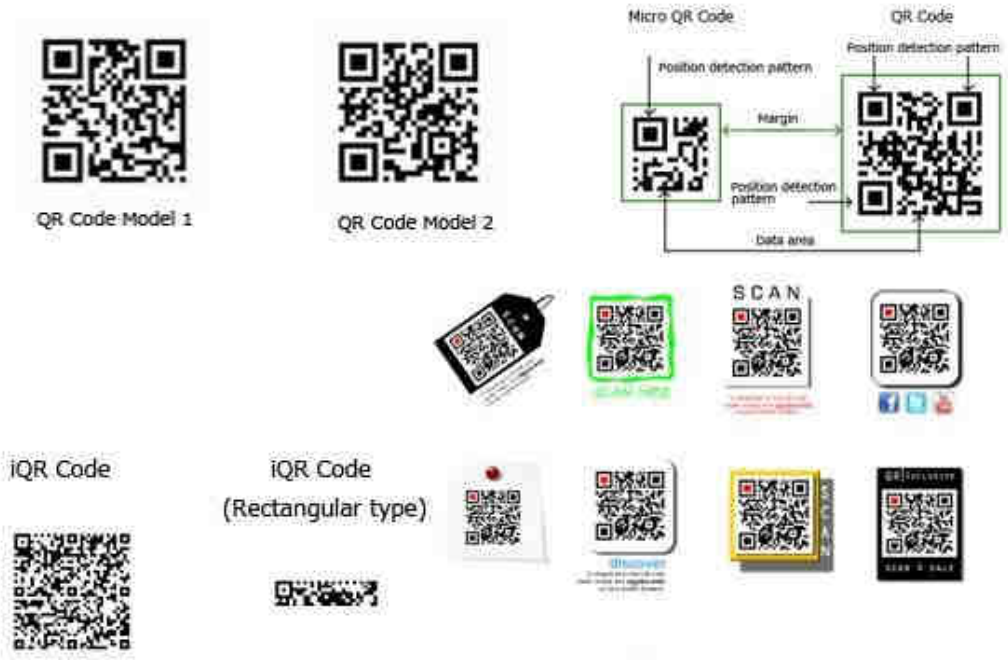
τις διαδικασίες και ρόλους που σχετίζονται με την ανακάλυψη Bluetooth συσκευών και τον διαχειρισμό της σύνδεσης τους.

Ανάλογα με την υλοποίηση ή/και την παραμετροποίηση, ρόλο κύριου controller μπορεί να έχει ο BR/EDR controller, ο οποίος περιλαμβάνει έλεγχο των radio, baseband, Link Manager και HCI, ο BLE controller, ο οποίος περιλαμβάνει το PHY, Link Layer και HCI και τέλος ο συνδυασμός τους.

2.7. Λειτουργία του QR Code

Το QR (Quick Response) Code, είναι ένα δισδιάστατο barcode το οποίο μπορεί να αποθηκεύσει πληροφορίες διάφορων ειδών όπως απλό κείμενο, σύνδεσμο, URL, SMS κείμενο, αριθμούς τηλέφωνου, συντεταγμένες, ακόμα και Kanji και kana χαρακτήρες. Πρώτη τους εμφάνιση έγινε στην αυτοκινητοβιομηχανία της Ιαπωνίας, όπου είχε σκοπό να επιτρέπει καλύτερο έλεγχο του inventory των διαφόρων τμημάτων των αυτοκινήτων. Έγινε όμως γρήγορα γνωστό έξω από την Ιαπωνία λόγω της γρήγορης ανάγνωσης που παρέχει και της μεγαλύτερης πληροφορίας που μπορεί να συγκρατήσει σε σχέση με το κλασσικό UPC barcode.

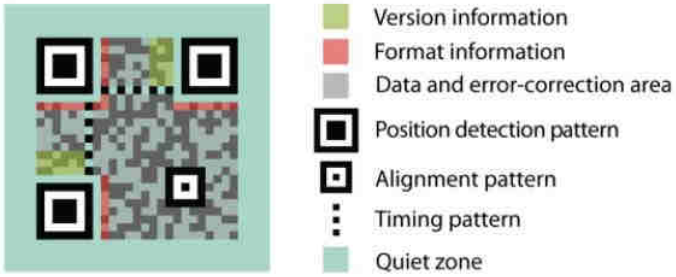
Μπορεί να κωδικοποιήσει πληροφορία τόσο σε οριζόντια όσο και κάθετη διεύθυνση, για αυτό και έχει πολλαπλάσια ικανότητα αποθήκευσης από τα UPC. Αποτελείται από άσπρα και μαύρα modules τα οποία αντιπροσωπεύουν την κωδικοποιημένη πληροφορία. Για να διαβαστεί η πληροφορία χρησιμοποιείται εξειδικευμένος αναγνώστης ή πλέον και ένα smartphone με την χρήση της κάμερας του και μιας QR code reader εφαρμογής. Υπάρχουν διάφοροι τύποι QR code οι οποίοι διαφέρουν κατά κύριο λόγο στην χωρητικότητα τους. Ακολουθούν εικόνες για διάφορους τύπους QR code **(εικόνα_11)**



Εικόνα 11 Τύποι QR-Code, by www.qrcode.com

Στα **model 1** έχουμε μέγιστη πληροφορία 1.167 αλφαριθμητικούς χαρακτήρες, στα **Module 2** φτάνουν και τους 7.089 και είναι και αυτά που συναντάμε κατά κύριο λόγο. Στα micro-QR απαιτείται μόνο μια διεύθυνση (οριζόντια ή κάθετη) για να αποτυπωθεί η πληροφορία, οπότε υπάρχει η δυνατότητα να έχουμε πολύ μικρότερης επιφάνειας κώδικα. Εδώ φτάνει το πολύ μέχρι 35 χαρακτήρες η πληροφορία. Οι **iQR** codes μπορούν να συγκρατήσουν πολύ περισσότερη πληροφορία στην ίδια επιφάνεια (έως και 80% περισσότερη) ή μπορούν την ίδια ποσότητα πληροφορίας να την αποτυπώσουν σε μικρότερη επιφάνεια από ένα κλασσικό QR code. Το πλέον εμφανές χαρακτηριστικό τους είναι ότι μπορούν να τυπωθούν και με οκταγωνικά Modules εκτός από τετράγωνα, πράγμα που τους επιτρέπει να αποτυπωθούν και σε κυλινδρικές επιφάνειες χωρίς να αλλοιώνεται η δυνατότητα να διαβαστούν σωστά. Τα **Frame QR** codes έχουν περισσότερο εμπορικό χαρακτήρα. Έχουν, συνήθως στο κέντρο τους κάποιο Logo ή σχέδιο ενώ ο κώδικας περιορίζεται στην περιφέρεια. Τέλος, υπάρχουν και τα **SQRC** codes, τα οποία δεν διαφέρουν εμφανισιακά με κάποιο από τα Module 2 QR codes, έχουν όμως το εξής χαρακτηριστικό, δεν επιτρέπουν την ανάγνωση από οποιαδήποτε συσκευή, περιορίζοντας έτσι την πρόσβαση σε συγκεκριμένο κύκλο ανθρώπων.

Στο παρακάτω σχήμα **(εικόνα_12)** φαίνονται τα χαρακτηριστικά ενός QR code,



Εικόνα 12 Χαρακτηριστικά QR-Code, wikipedia

- **Position Detection**, αυτά τα πανομοιότυπα τμήματα τοποθετημένα στις τρεις γωνίες του QR, έχουν τον ρόλο να ορίζουν στο software ενός αναγνώστη QR code τα όρια του χώρου που βρίσκεται ο κώδικας. Αυτά είναι που δίνουν την δυνατότητα να αναγνωστεί το QR από 360 μοίρες.
- **Timing**, μια αλληλουχία από άσπρα και μαύρα Modules που βοηθάνε να διευκρινιστεί από τον αναγνώστη το πλάτος ενός module
- **Alignment**, αυτό το pattern εμφανίζεται από την version 2 και πάνω και βοηθάει τον αναγνώστη του QR να μην χάνει τον προσανατολισμό του εάν η επιφάνεια του QR έχει καμφθεί ή είναι απλά σε καμπύλη επιφάνεια.
- **Format Information**, αποτελείται από 15 bits πληροφορία και ενημερώνει για τον τύπο του error correction και το mask pattern (αν υπάρχουν)
- **Data & Error Correction Data**, περιλαμβάνει τόσο τα κανονικά δεδομένα όσο και αυτά που χρησιμεύουν για την διαδικασία του error correction

Επειδή τμήμα της επιφάνεια του κωδικού μπορεί να καταστραφεί, εισάγεται μία δικλείδα ασφάλειας που ονομάζεται κώδικας διόρθωσης σφάλματος Reed-Solomon (16)**.** Η δυνατότητα του κώδικα αυτού να διατηρήσει την συνοχή ενός QR code ύστερα από ζημία στην επιφάνεια του εξαρτάται άμεσα από την μέγιστη πληροφορία που μπορεί να αποτυπωθεί πάνω στο QR code. Το στοιχείο του Reed-Solomon χρειάζεται να διαθέτει την διπλάσια ποσότητα πληροφορίας από την μέγιστη πληροφορία που θα κληθεί να διορθώσει. Αν δηλαδή, αχρηστευτούν από ζημιά 50 codewords, το Reed-Solomon τμήμα θα πρέπει να έχει τουλάχιστον 100 codewords. Οπότε, όσο μεγαλύτερη η δυνατότητα για διόρθωση σφάλματος τόσο μικρότερη η πληροφορία που μπορεί να αποθηκευτεί στα QR. Για την ώρα υπάρχουν τέσσερα διαφορετικά επίπεδα διόρθωσης στα 7%, 15%, 25% και τέλος 30% ζημιάς που μπορεί να διαχειριστεί.

2.8. Λειτουργία Βιομετρικών

2.8.1. Εισαγωγή

Ως βιομετρικά, ορίζονται τα μετρικά συστήματα που σχετίζονται με τα ανθρώπινα χαρακτηριστικά. Αποτελεί απόλυτα ελληνική λέξη και προέρχεται από τα συνθετικά *βίος* (ζωή) και *μετρικός* (μέτρο). Η χρήση των βιομετρικών στηρίζεται στην αρχή του "Τι Είμαι", σε αντίθεση με το "Τι Γνωρίζω" (PIN) και "Τι Έχω" (κάρτα). Τα βιομετρικά συστήματα επομένως, είναι συστήματα αναγνώρισης ενός μοτίβου/πρότυπου, τα οποία αναγνωρίζουν ένα άτομο βάση ενός συγκεκριμένου χαρακτηριστικού φυσιολογίας ή/και συμπεριφοράς που έχει το άτομο. Ανάλογα δε με τον τρόπο που θα υλοποιηθεί, γίνονται διακριτές 2 μορφές λειτουργίας, η ταυτοποίηση (**identification**), που απαντά στην ερώτηση "ποιος είμαι?" και η εξακρίβωση (**verification**), που απαντά στην ερώτηση "είμαι αυτός που ισχυρίζομαι?".

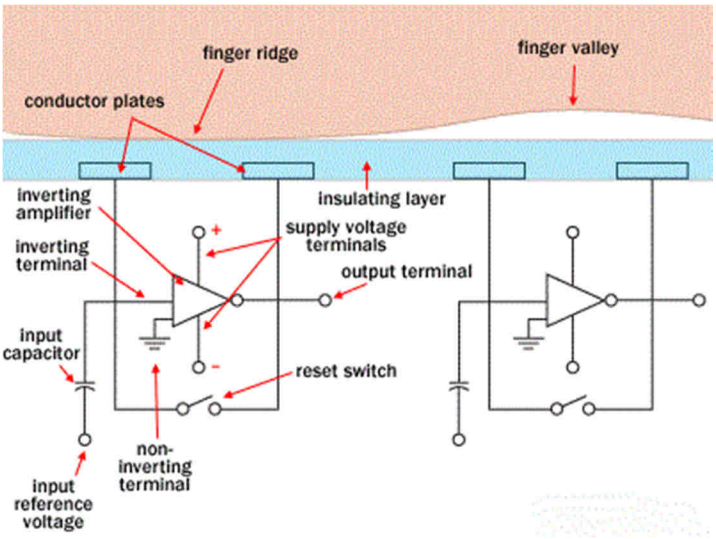
Στις ενότητες που ακολουθούν θα γίνει αναφορά και παρουσίαση στα είδη των βιομετρικών που έχουν το μεγαλύτερο μερίδιο στην αγορά του Security και εμφανίζονται κατά κύριο λόγω στα συστήματα των mobile wallets που θα παρουσιαστούν παρακάτω.

2.8.2. Δακτυλικό αποτύπωμα.

Από τα πρώτα βιομετρικά που χρησιμοποιήθηκαν ήταν το δακτυλικό αποτύπωμα. Στην σύγχρονη ιστορία, πρώτη καταγεγραμμένη αναφορά έγινε από τον καθηγητή John Evangelist Purkinje το 1823 (17) όπου στην έρευνα που κυκλοφόρησε έκανε αναφορά για 9 patterns δακτυλικών αποτυπωμάτων. Το1892 έγινε η πρώτη αναγνώριση εγκληματία μέσω αποτυπώματος, ενώ πλέον σήμερα, η εξέλιξη έχει φτάσει στο AFIT (18) (advanced fingerprint identification technology), μια μέθοδο που αναπτύχθηκε από το F.B.I και εφαρμόστηκε πρώτη φορά τον Φλεβάρη του 2015, βελτιώνοντας το ποσοστά επιτυχής διασταύρωσης των αποτυπωμάτων από 92% σε σχέση με το προηγούμενο σύστημα τους σε 99.6%. Το δακτυλικό αποτύπωμα είναι ένα βιομετρικό που δύσκολα αλλάζει με την ηλικία, εκτός και εάν στο δάκτυλο προκληθεί ζημιά από κάποιο ατύχημα ή ασθένεια ή απλά από χρόνια φθορά λόγω συγκεκριμένου τύπου εργασίας. Χαρακτηρίζεται από μία σειρά γραμμών (ridges), ξεχωριστή για κάθε άνθρωπο, και τα κενά που δημιουργούνται από αυτές τις γραμμές(valleys).

Στο εμπόριο βρίσκονται δύο τύποι scanner για δακτυλικά αποτυπώματα, οπτικοί όπου η ανίχνευση γίνεται μέσω φωτισμού και capacitance όπου χρησιμοποιείται ηλεκτρικό ρεύμα και είναι και οι πιο διαδεδομένοι πάνω στο αντικείμενο απασχολεί αυτή την ανάλυση. Στο σχήμα

που ακολουθεί φαίνεται πως λειτουργεί ένας capacitance scanner **(εικόνα_13)**. Η επιφάνεια του scanner αποτελείται από μονωτικό υλικό και εκεί κάνει επαφή το δάκτυλο. Κάτω ακριβώς από αυτό το υλικό υπάρχουν ένα ή περισσότερα ημιαγώγιμα chips, τα οποία διαθέτουν μία σειρά από cells, καθένα από τα οποία είναι μικρότερα από το πλάτος μιας γραμμής του αποτυπώματος μας. Το κάθε cell, διαθέτει 2 αγώγιμες επιφάνειες. Οι επιφάνειες αυτές είναι που σχηματίζουν τον πυκνωτή στον οποίο αποθηκεύεται το ρεύμα. Μόλις το δάκτυλο πιέσει στην επιφάνεια, λειτουργεί σαν τρίτη επιφάνεια πυκνωτή και επειδή η απόσταση αλλάζει χωρητικότητα, η τάση που θα προκύψει θα είναι διαφορετική αν έχουμε ridge ή valley. Οπότε, το scanner διαβάζει την είσοδο σε ρεύμα από κάθε cell, καταλαβαίνει αν πρόκειται για ridge ή valley και αθροίζοντας τις εισόδους από όλα τα cells, καταλήγει σε μία εικόνα του δακτυλικού αποτυπώματος.



Εικόνα 13 Μοντέλο Λειτουργίας Capacitance Scanner, by How Stuff Works

Μόλις το μοντέλο του αποτυπώματος δημιουργηθεί, χρησιμοποιούνται πολύπλοκοι αλγόριθμοι για να συγκρίνουν χαρακτηριστικά του αποτυπώματος (Minutiae) (19) με εκείνου που έχει ήδη στην βάση του για να προκύψει πιστοποίηση ή μη του δείγματος. Τα σημεία που ελέγχονται είναι συνήθως εκεί που τελειώνει ένα Ridge ή εκεί που διακλαδίζονται (Bifurcation). Οι αλγόριθμοι που χρησιμοποιούνται είναι pattern-based, και απαιτείται οι εικόνες να έχουν την ίδια κατεύθυνση, γι’ αυτό οι αλγόριθμοι βρίσκουν ένα κεντρικό σημείο στην εικόνα και επικεντρώνονται εκεί.

2.8.3. Αναγνώριση Φωνής

Ενώ όμως υπάρχει πληθώρα υλοποιήσεων από βιομετρικά αντίμετρα με τη χρήση του δακτυλικού αποτυπώματος, έδαφος έχει αρχίσει να κερδίζει και η χρήση της φωνής ως μέσο πρόσβασης και αυθεντικοποίησης. Αργότερα κατά την παρουσίαση των Mobile wallets, υπάρχει και μία υλοποίηση με voice recognition, αλλά πρώτα θα παρουσιαστούν τα βασικά χαρακτηριστικά αυτής της μεθόδου.

Αρχικά, υπάρχει σαφής διαχωρισμός μεταξύ του όρου "**αναγνώριση φωνής**" (ικανότητα να ξεχωρίσουμε τα βιολογικά χαρακτηριστικά της φωνής) και του όρου "**αναγνώριση ομιλίας**", όπου αναγνωρίζει λέξεις καθώς αυτές διατυπώνονται (20), το οποίο δεν θεωρείται βιομετρικό χαρακτηριστικό. Στο αντικείμενο του authentication το ενδιαφέρον εστιάζεται στην μέθοδο της αναγνώρισης φωνής. Οι δύο κυριότερες υλοποιήσεις της αναφορικά με θέματα ασφάλειας είναι η ταυτοποίηση (**identification**), που απαντά στην ερώτηση "ποιος είμαι?" και η εξακρίβωση (**verification**), που απαντά στην ερώτηση "είμαι αυτός που ισχυρίζομαι?". Στην πρώτη περίπτωση, ο cardholder **δεν** ισχυρίζεται ότι είναι κάποιος, οπότε το σύστημα ελέγχει τις βάσεις του και προσπαθεί να ταυτίσει χαρακτηριστικά από τα δείγματα που έχει μέσα με αυτά του χρήστη, όπου μπορεί να έχει "match" ή "no match". Στο σενάριο της εξακρίβωσης, το σύστημα κάνει σύγκριση των χαρακτηριστικών του χρήστη, με ένα μόνο template της βάσης (που θεωρητικά είναι του χρήστη) και ανάλογα με το αν έχουμε ή όχι ταύτιση έχουμε ένδειξη "true" ή "false".

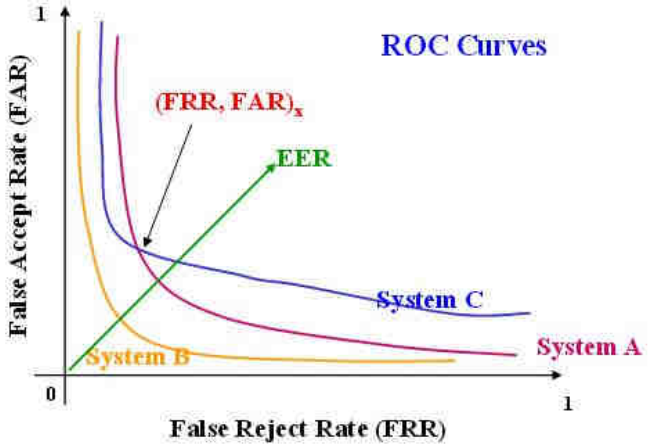
2.8.4. Δείκτες Μέτρησης

Όπως και στα δακτυλικά αποτυπώματα, υπάρχουν η φάση της καταχώρησης δείγματος και η φάση της εξακρίβωσης. Στην περίπτωση όπου χρειάζεται το κείμενο ομιλίας να είναι ίδιο στην εξακρίβωση με αυτό της καταχώρησης, είναι η λεγόμενη **Text-Dependent** αναγνώριση. Ως κείμενο δύναται να οριστεί κάποιο password ή PIN ώστε να υπάρχει **two-factor authentication**. Εάν αντίθετα, το κείμενο δεν χρειάζεται να ταυτίζεται στην καταχώρηση με την αναγνώριση, η διαδικασία εξακρίβωσης ονομάζεται Text-Independent (21). Από τις επικρατέστερες μεθόδους που υλοποιούνται οι μηχανισμοί φωνητικής αναγνώρισης, είναι τα μοντέλα **Hidden Markov** (22)**,** τα οποία αποτελούν στατιστικά μοντέλα με τα οποία το σύστημα παρακολουθεί μια σειρά από φωνητικές καταχωρήσεις, χωρίς να ξέρει την σειρά με την οποία πραγματοποιήθηκαν και

προσπαθεί να καταλήξει μέσα από αλγορίθμους, σε μία στατιστική αναπαράσταση του πως ο cardholder μιλάει (παράγει ήχο).

Για την μέτρηση της απόδοσης ενός βιομετρικού συστήματος, χρησιμοποιούνται μια σειρά από δείκτες. (23)

- F.A.R, False Accept rate, είναι το σφάλμα σε ποσοστό % όταν ένα λάθος βιομετρικό δείγμα γίνεται δεκτό ως σωστό
- F.R.R, False Reject Rate, είναι το σφάλμα σε ποσοστό % όταν ένα σωστό βιομετρικό δείγμα απορρίπτεται ως λάθος
- R.O.C, Receiver Operating Characteristic, είναι η γραφική παράσταση **(εικόνα_14)** που προκύπτει από την απεικόνιση των F.A.R και F.R.R πάνω σε άξονες και χρησιμεύει είτε για την σύγκριση συστημάτων ή για την διαμόρφωση τους.
  (παράδειγμα, όταν εφαρμόζονται σε χώρους ή συστήματα υψηλού ρίσκου, το σύστημα ρυθμίζεται έτσι ώστε να έχει υψηλότερο FRR και ας προκαλεί δυσανασχέτηση). Η τιμή EER σημαίνει Equal Error Rate, και δείχνει το σημείο στο οποίο τα δύο ποσοστά F.A.R και F.R.R ταυτίζονται. Όσο πιο χαμηλό, τόσο πιο αποτελεσματικό το βιομετρικό σύστημα.



Εικόνα 14 Γράφημα ROC, Performance Measure in Biometric Systems, 2006

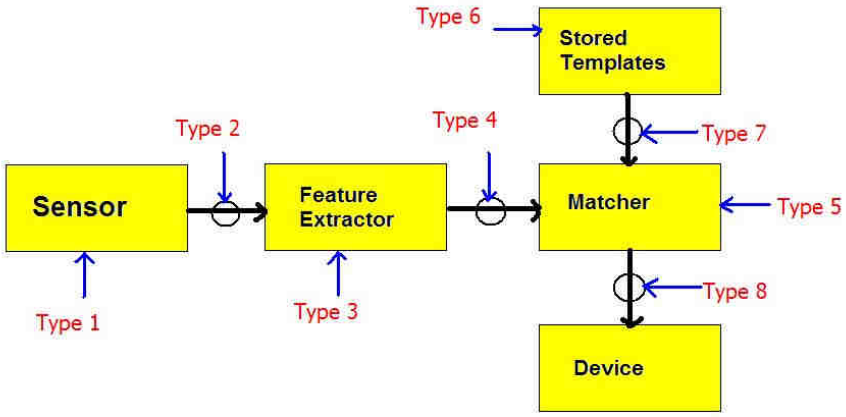
- F.T.C, Failure to Capture, είναι το ποσοστό των φορών όπου το βιομετρικό σύστημα δεν κατάφερε (για τον οποιοδήποτε λόγο) να πάρει το δείγμα.

- F.T.E, Failure to Enroll, το ποσοστό των περιπτώσεων όπου υπάρχει αποτυχία στην εισαγωγή νέου βιομετρικού χαρακτηριστικού για καταχώρηση στην βάση, λόγω κακής ποιότητας του δείγματος.

2.8.5. Εξέλιξη-Προβλήματα-Λύσεις

Τα βιομετρικά έχουν αρχίσει να έχουν μεγάλη άνθιση ως μέσω αυθεντικοποίησης, ειδικά στον τραπεζικό κλάδο αλλά και στις εγχρήματες συναλλαγές. Το μεγάλο τους κόστος έχει πάψει πλέον να είναι θέμα καθώς κάθε αξιοπρεπής smartphone συσκευή πλέον, είναι εξοπλισμένη με ότι χρειάζεται σε θέμα hardware για να πραγματοποιήσει αναγνώριση φωνής, ίριδας, προσώπου και δακτυλικού αποτυπώματος. Από το 2002 και μετά άρχισαν να γίνονται και οι πρώτες σοβαρές απόπειρες για την δημιουργία κανονιστικών και τεχνικών πλαισίων, όπως το ISO/IEC JTC 1/SC 37 και ακολουθούν οι NIST και BSI. Προκύπτουν όμως θέματα νομικής (privacy) αλλά και χρηστικής φύσης καθώς τα βιομετρικά αποτελούν PII δεδομένα (24) και η τυχόν υποκλοπή τους από βάσεις δεδομένων θα αποτελούσε πλήγμα πολύ μεγαλύτερο από την υποκλοπή πιστωτικών καρτών, καθώς, ειδικά στην Ευρώπη, υπάρχουν πολύ αυστηροί κανονισμοί για θέματα προσωπικών δεδομένων, όπως αυτοί που επιβάλλονται από την GDPR (European General Data Protection Regulation). Επιπλέον, σημαντικό αντικίνητρο είναι ότι, ότι σε αντίθεση με τα κλασσικούς τρόπους αυθεντικοποίησης όπως ένα PIN, τα βιομετρικά χαρακτηριστικά δεν αλλάζουν. Εάν διαρρεύσει ένα PIN μπορεί να αλλάξει, αν χαθεί μια κάρτα μπορώ να ακυρωθεί, αλλά το δακτυλικό αποτύπωμα ή την ίριδα του ματιού, είναι χαρακτηριστικά που μένουν ίδια. Επιπλέον, υπάρχει μια γενική ανησυχία για την ποσότητα και ποιότητα των προσωπικών δεδομένων που συγκεντρώνονται ανά άτομο όπως, όνομα, ηλικία, διεύθυνση οπότε με την προσθήκη σε αυτά και χαρακτηριστικών που μας κάνουν απόλυτα διακριτούς, τίθενται θέματα για το που μπορεί να χρησιμοποιηθούν και κατά πόσο προστατεύονται.

Στο σχήμα που ακολουθεί **(εικόνα_15)** φαίνονται τα σημεία που μπορεί να πραγματοποιηθούν επιθέσεις σε ένα κοινό βιομετρικό σύστημα. Ακολουθούν οι πιο χαρακτηριστικές επιθέσεις που μπορούν γίνουν σε κάθε ένα από τα σημεία.



Εικόνα 15 Σημεία Επίθεσης σε Βιομετρικό Σύστημα, by McMaster Uni

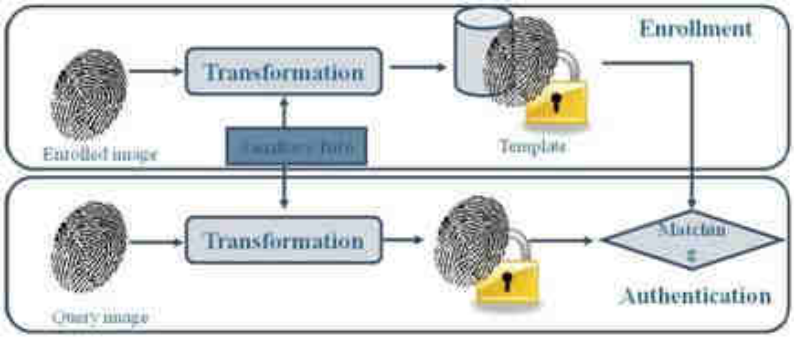
1. Παρουσίαση πλαστού δείγματος, όπως ψεύτικο δάκτυλο, copy υπογραφής, μάσκα αντί για κανονικό πρόσωπο. Υπάρχει δε και η περίπτωση να γίνει παραποίηση του ίδιου του αισθητήρα για υποκλοπή ενός πραγματικού δείγματος κατά την εισαγωγή του.
2. Replay επίθεση, με την παρουσίαση, για παράδειγμα, ηχογραφημένου μηνύματος ή εικόνας δακτυλικού αποτυπώματος ή προσώπου.
3. Σε αυτό το σημείο είναι δυνατόν, με την χρήση πχ Trojan, να γίνεται επιλογή συγκεκριμένων χαρακτηριστικών που έχει επιλέξει ο επιτιθέμενος για προώθηση προς έλεγχο.
4. Αυτή η επίθεση είναι πολύ δύσκολο να πραγματοποιηθεί αλλά όχι αδύνατον. Συνήθως το feature extraction και matching γίνονται σε έναν χρόνο, αλλά στην περίπτωση που έχουμε online authentication και στέλνονται σε online matcher για επιβεβαίωση, δύναται να υποκλαπεί η κίνηση των πακέτων στο tcp/ip και να αντικατασταθούν τα πραγματικά δεδομένα που στάλθηκαν με ψεύτικα. Μπορεί ακόμα να πραγματοποιηθεί και DOS (denial of service) επίθεση, μη επιτρέποντας την πρόσβαση στο σύστημα.
5. Και πάλι εδώ, μπορεί να υπάρξει tampered matcher με κάποιο Trojan και να παρουσιάζει προεπιλεγμένες επικυρώσεις.
6. Παραποίηση στην βάση δεδομένων, αλλοιώνοντας τα templates των πραγματικών δειγμάτων, δίνοντας πιστοποίηση σε κάποιον που δεν θα έπρεπε ή αντίθετα, απαγορεύοντας την πρόσβαση σε κάποιον που την δικαιούται.

7. Αντί για επίθεση στην ίδια την βάση, αυτή την φορά γίνεται επίθεση στο κανάλι που συνδέει την βάση με τον matcher.
8. Στην τελική έξοδο, μπορεί να πραγματοποιηθεί παράκαμψη της όλης διαδικασίας, αλλοιώνοντας το τελικό αποτέλεσμα, χωρίς να γίνει επέμβαση σε κανένα από τα προηγούμενα βήματα. Οπότε, ενώ το σύστημα μπορεί να έχει παρουσιάσει άψογη συμπεριφορά, και να παρουσιαστεί αντίθετο αποτέλεσμα από το αναμενόμενο.

Οι επιθέσεις που παρατηρούνται, δεν διαφέρουν πολύ σε μεθοδολογία από αυτές που έχουν εμφανιστεί σε password-based περιβάλλον. Ακόμα και οι τεχνικές αντιμετώπισης είναι μέχρι ένα σημείο κοινές, για παράδειγμα, στο σημείο 4 θα μπορούσε να υπάρχει προστασία από κρυπτογραφημένα κανάλια επικοινωνίας, ενώ για τα σημεία 5,6 και 7 θα μπορούσε να τοποθετηθούν σε προστατευμένο σημείο (βλέπε Secure Element στα κινητά).

Πάνω σε αυτή τη νοοτροπία, εισήχθη η ιδέα των cancelable βιομετρικών (25). Πρόκειται για μία εσκεμμένη, επαναλαμβανόμενη αλλοίωση του κανονικού βιομετρικού δείγματος με συγκεκριμένη μέθοδο. Το κάθε δείγμα, παραμορφώνεται με τον ίδιο τρόπο τόσο στην εισαγωγή του στην βάση όσο και κάθε φορά που παρουσιάζεται για αυθεντικοποίηση. Εάν μια παράμετρος της αλλαγής αποκαλυφθεί, μπορεί απλά να αλλάξει η συνάρτηση που κάνει την μετατροπή, οπότε με την ίδια πηγή βιομετρικού προκύπτει διαφορετικό αποτέλεσμα και κατά συνέπεια θα διατηρείται η μη δυνατότητα απόδοσης του βιομετρικού στον άνθρωπο που ανήκει. Σαν τακτική πάντως, οι συναρτήσεις που χρησιμοποιούνται για την παραμόρφωση του δείγματος, είναι μη αναστρέψιμες, οπότε, ακόμα και αν διαρρεύσει τόσο το παραμορφωμένο δείγμα όσο και η συνάρτηση που πραγματοποίησε την αλλαγή, δεν θα μπορεί κάποιος να ανακτήσει το αρχικό δείγμα.

Η μέθοδος που χρησιμοποιείται κατά κύριο λόγω είναι το **Biometric Salting(εικόνα_16)**. Όπως και στην κρυπτογραφία, κατά την είσοδο του βιομετρικού δείγματος, εισάγεται μία τυχαία ποσότητα από r bits σε συνδυασμό με ένα μυστικό κλειδί k. Το αποτέλεσμα αποθηκεύεται στην βάση δεδομένων ως ένα hash H(r+k). Η έξτρα πληροφορία που δημιουργείται για τις ανάγκες του salting, μπορεί να αναιρεθεί ή να αλλάξει αν κριθεί ότι δεν είναι αρκετή ή επισφαλής, καθώς έχει αναγνωριστεί ότι δύναται να έχει τις ίδιες αδυναμίες με αντίστοιχες υλοποιήσεις όπου χρησιμοποιείται hashing και κλειδιά για κρυπτογράφηση.



Εικόνα 16 Biometric Salting, by Scholarpedia-Salting

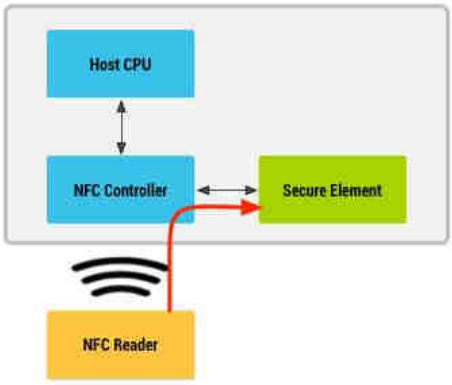
Ακόμα δεν υπάρχει κάποιο ευρέος αποδεκτό standard για την μεθοδευμένη χρήση τους από την βιομηχανία, το οποίο να περιλαμβάνει όλη την αλυσίδα: service enrollment, χρήση, μετάδοση δεδομένων, αποθήκευση. Επίσης, η αποκλειστική τους χρήση για authentication δεν είναι αρκετή, πλέον το two-factor authentication θεωρείται απαραίτητο. Παρόλα αυτά, νέες εφαρμογές τους συνεχίζουν να αναπτύσσονται, όπως το finger-vein recognition, μια τεχνολογία που αναπτύχθηκε και υλοποιήθηκε από την Hitachi και έχει ήδη αρχίσει να προωθείται σε ATMs της Ινδίας, Πολωνίας και Ιαπωνίας. Στο πλαίσιο της έρευνας, έχουν γίνει προσπάθειες για την υλοποίηση λύσεων δευτερευόντων βιομετρικών όπως φύλλο, ηλικία, ύψος και χρώμα δέρματος, λεγόμενα και **soft biometrics** (26), αλλά τέθηκαν προβληματισμοί για θέματα διακρίσεων και ρατσισμού που μπορεί να προκύψουν.

2.9. Λειτουργία Host Card Emulation

Ο όρος HCE, χρησιμοποιείται για μα περιγράψει την software αρχιτεκτονική η οποία δημιουργεί ένα ασφαλές κανάλι επικοινωνίας ανάμεσα σε ένα NFC enabled POS τερματικό και ένα απομακρυσμένο Payment network (27)**,** χρησιμοποιώντας ως proxy μία φορητή συσκευή χωρίς φυσικό secure element. Η αρχιτεκτονική αναπτύχθηκε από την εταιρία SimplyTap το 2012 και ενσωματώθηκε από την Google σχεδόν άμεσα καθώς το ενσωμάτωσε στην έκδοση 4.4 του Android και όλες τις μεταγενέστερες. Σύντομα, υποστηρίχθηκε τόσο από την Visa όσο και την Mastercard.

Για την υλοποίηση αυτής της αρχιτεκτονικής, απαιτείται η χρήση του NFC πρωτοκόλλου. Το NFC, όπως αναφέρθηκε και στην περιγραφή του, έχει ένα Mode λειτουργίας που ονομάζεται card emulation mode. Αυτό επιτρέπει στην συσκευή να συμπεριφέρεται ως NFC κάρτα και να είναι αναγνώσιμη από ένα NFC enabled POS. Η προσομοίωση αυτή γινόταν με

την αρωγή ενός secure element επάνω στη συσκευή στο οποίο και αποθηκεύονταν στοιχεία της κάρτας (debit, visa κα), ενώ σε παλαιότερες υλοποιήσεις, τον ρόλο του SE τον είχε η κάρτα SIM. Ο cardholder κρατούσε την συσκευή πάνω από το POS**(εικόνα_17)**, ο NFC reader προωθούσε τα στοιχεία της συναλλαγής στον NFC controller της συσκευής και από εκεί στο SE. Αυτό με τη σειρά του "μίλαγε" απευθείας με τον NFC reader του POS, χωρίς την συνδρομή κάποιου API (28)**.**



Εικόνα 17 Λειτουργία NFC με SE, by Android-Developer guide

Με την υλοποίηση του HCE, ο NFC reader του POS μιλάει, μέσω του NFC controller της συσκευής, με ένα Wallet App (το οποίο διαχειρίζεται τις κάρτες) και τα HCE services. Επειδή η επικοινωνία δεν γίνεται μέσα από κάποιο hardware SE, υπάρχει το πλεονέκτημα ότι δεν χρειάζεται στη διαδικασία να ληφθεί υπόψη η αρχιτεκτονική της συσκευής (κάθε συσκευή έχει το δικό της SE), ούτε ο πάροχος του δικτύου επικοινωνίας (ο οποίος αρκετές φορές παρέχει την συσκευή), οπότε, οντότητες όπως οι MNO και OEM, βγαίνουν από το "οικοσύστημα" του συστήματος mobile πληρωμών. Το ίδιο μπορεί να ειπωθεί και για την ανάγκη να έχουν ρόλο TSM οι οντότητες Issuer και MNO.

Τα δομικά στοιχεία που είναι απαραίτητα για την υλοποίηση συστήματος πληρωμών μέσω φορητής συσκευής με την χρήση HCE είναι ενδεικτικά τα εξής (29):

- Cloud-Based πλατφόρμα πληρωμών. Εφόσον οι λογαριασμοί των Cardholders για τις συναλλαγές τους θα βρίσκονται στο Cloud, απαιτείται και το αντίστοιχο πρόγραμμα διαχείρισης τους. Οι πλατφόρμες αυτές θα διαχειρίζονται από τους Issuers ή από 3rd parties. Στις δυνατότητες τους θα μπορούν να περιλαμβάνουν, διαχείριση των PAN αριθμών και επικύρωση των μεθόδων CVM.

- Εφαρμογή των πληρωμών-Wallet. Θα είναι ο ενδιάμεσος κρίκος ανάμεσα στον Cardholder και την πλατφόρμα πληρωμών. Θα παρέχει το interface μέσα από το οποίο θα πραγματοποιείται η εγγραφή του πελάτη στην εκάστοτε υπηρεσία πληρωμών (πχ Apple Pay). Η εφαρμογή θα ανήκει είτε στον Issuer είτε, όπως θα δούμε και παρακάτω, στον προμηθευτή των συσκευών και θα πρέπει να παρέχει ασφαλή επικοινωνία με την πλατφόρμα πληρωμών.
- Token Service Provider: όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, ο ρόλος του TSP είναι εξαιρετικά σημαντικός για την επιτέλεση του tokenization και την προκάλυψη του πραγματικού αριθμού της κάρτας. Στην υλοποίηση με HCE τον ρόλο θα μπορεί να τον αναλάβει το Payment Network.

Επειδή στην υλοποίηση του HCE δεν υπάρχει hardware SE, η αποθήκευση δεδομένων αναφορικά με mobile πληρωμές στην συσκευή θα πρέπει να πραγματοποιηθεί μέσα από πολλαπλά επίπεδα, στον τομέα της εφαρμογής, της επικοινωνίας και της ίδιας της συσκευής. Αυτό που αποτελεί την μεγαλύτερη απειλή είναι η κλοπή του token. Ήδη έγινε αναφορά για την τεχνική του tokenization σε προηγούμενο κεφάλαιο και την παγίωση της υλοποίησης του με την χρήση δυναμικών δεδομένων έναντι των σταθερών. Έτσι, ακόμα και αν κλαπεί το token, θα αποφευχθεί τυχόν replay attack καθώς θα είναι άχρηστο για μελλοντικές συναλλαγές και το πραγματικό token δεν θα μπορεί να ανασυρθεί. Παλιότερες προτάσεις ανάφεραν έκδοση διαφορετικού PAN για την κάθε συναλλαγή, αλλά κατέληξαν ότι πιο πρακτικό σε θέματα διαχείρισης και ταχύτητας να υπάρχει ένα τροποποιημένο PAN(token) σε συνδυασμό με ένα είδους cryptogram (αναφέρετε σε βιβλιογραφίες και ως session key). Ανεξαρτήτως υλοποίησης του tokenization, τα τρία επίπεδα που αναφέρθηκαν παραπάνω, οφείλουν να παρέχουν την μέγιστη δυνατή ασφάλεια στα δυναμικά δεδομένα που μεταφέρονται και ενίοτε αποθηκεύονται στην συσκευή.

Στον τομέα της Ασφάλειας της Εφαρμογής, σημαντικό σημείο είναι η ασφαλής διαχείρισης των κλειδιών και των προσωπικών δεδομένων που υπάρχουν στην συσκευή και χρησιμοποιούνται από την εφαρμογή πληρωμής. Σημαντικό λοιπόν είναι να υπάρχει περιβάλλον TEE όπου θα επιτρέπει την ασφαλή αποθήκευση και μεταφορά κρυπτογραφικών κλειδιών και πληροφορίας. Τέτοια υπηρεσία παρέχει η υλοποίηση της Samsung με την πλατφόρμα Knox που θα αναλυθεί παρακάτω.

Αντίστοιχα, στο θέμα της Ασφάλειας της συσκευής, είναι υψίστης σημασίας να μπορεί το σύστημα να επαληθεύσει ανά πάσα στιγμή την ακεραιότητα της συσκευής λόγω έλλειψης hardware SE. Και πάλι μια τέτοια υλοποίηση προσφέρεται από την Samsung στο Samsung Pay μέσω της διαδικασίας TIMA Attestation, η οποία θα αναλυθεί με περισσότερη λεπτομέρεια σε παρακάτω κεφάλαιο.

Τέλος, ας μην παραλειφθεί, η σημασία της ασφαλής επικοινωνίας μεταξύ της εφαρμογής πληρωμής πάνω στη συσκευή και του cloud πλέον SE, για την αδιάλειπτη μεταφορά του πακέτου πληροφορίας που είναι το token και τα δυναμικά δεδομένα μαζί με τα δεδομένα της πληρωμής. Αυτό συνήθως επιτυγχάνεται με ισχυρή κρυπτογραφία πάνω στους δίαυλους επικοινωνίας με την χρήση πχ SSL τεχνολογίας.

Η λύση του HCE προσφέρει αρκετά στρατηγικά πλεονεκτήματα και χώρο για ευελιξία αλλά η έλλειψη hardware SE ανεβάζει τον πήχη σε απαιτήσεις ασφάλειας σε όλα τα επίπεδα καθώς πλέον η ασφάλεια κεντρικοποιείται εφόσον βγαίνουν εκτός αρχιτεκτονικής συστήματος οι δύο οντότητες που προσφέρουν hardware υλοποιήσεις (MNO & OEM), αλλά από την άλλη ένα ρήγμα στο κομμάτι του cloud θα προκαλέσει μαζική διαρροή δεδομένων σε αντίθεση με μια επίθεση σε κινητή συσκευή.

3. Απειλές στις οποίες είναι Ευάλωτο το σύστημα των Mobile Wallets

Η χρήση των κινητών συσκευών στον χώρο των εγχρήματων συναλλαγών, εισάγει νέες απειλές που οφείλονται κατά κύριο λόγο στην ευάλωτη φύση τους. Τα κινητά άλλωστε, έχουν πλέον εξελιχθεί σε υπολογιστές τσέπης με δυνατότητα σύνδεσης στο δίκτυο, οπότε, παρουσιάζουν πολλά κοινά προβλήματα με τα κανονικά pc όπως viruses, malwares και phishing attacks. Οι πιο ενδεικτικές απειλές, παρουσιάζονται σε αυτή την ενότητα.

3.1. Mobile Malware

Ως malware (malicious software) περιγράφετε το σύνολο των κακόβουλων προγραμμάτων που χρησιμοποιούνται για να διαταράξουν την ομαλή λειτουργία των υπολογιστών, την κλοπή προσωπικών δεδομένων, την απόκτηση απαγορευμένων προσβάσεων και γενικότερα την πρόκληση ζημιάς στα πληροφοριακά συστήματα είτε απλών χρηστών είτε κυβερνητικών οργανισμών και επιχειρήσεων. Εμφανίζεται με διάφορες μορφές εκτελέσιμου κώδικα, scripts, active content και σε διάφορες classes. Πάνω από 317 εκατομμύρια νέα malwares εμφανίστηκαν μόνο μέσα στο 2014, σχεδόν 1 εκατομμύριο την ημέρα, μια αύξηση της τάξης του 26% σε σχέση με το 2013 (30). Ειδικά στην υποκατηγορία των mobile malwares, είχαμε 5% επιπλέον αύξηση το 2014 σε σχέση με το 2013. Έξι από τα είκοσι πιο επιζήμια mobile malwares, ανήκαν στα spyware, κακόβουλο λογισμικό με ειδίκευση να εντοπίζει γεωγραφική θέση της συσκευής και εισερχόμενα και εξερχόμενα μηνύματα και κλήσεις. Ακολουθούν οι βασικότερες μορφές που εμφανίζονται.

3.1.1. Viruses and Worms

Οι ιοί, αποτελούν κακόβουλο λογισμικό με την ιδιότητα να δημιουργούν αυτόματα αντίγραφα του εαυτού τους και μολύνουν λογισμικό το οποίο υπό νορμάλ συνθήκες είναι εγκεκριμένο προς χρήση. Συνήθως είναι ενσωματωμένοι πάνω σε κάποιο εκτελέσιμο αρχείο το οποίο μόλις εκτελεστεί ενεργοποιεί τον ιό ο οποίος με την σειρά του εξαπλώνεται στο σύστημα είτε σε άλλα προγράμματα, είτε σβήνοντας αρχεία ή απλά (και ανάλογα τον προγραμματισμό του) εισχωρεί σε προγράμματα ηλεκτρονικού ταχυδρομείου ώστε να εξαπλωθεί και σε άλλα τερματικά συστήματα. Τα Worms, αποτελούν μία πιο εξελιγμένη μορφή ιών, καθώς λειτουργούν αυτόνομα, χωρίς την ανάγκη να ενσωματωθούν σε κάποιο εκτελέσιμο ή πρόγραμμα για να κινηθούν στο δίκτυο.

Το worm με την κωδική ονομασία *Gazon*, είναι από τα πλέον υποδειγματικά παραδείγματα malware. Μεταδίδεται μέσω sms μηνυμάτων, με ένα μικρό Link το οποίο κάνει τον χρήστη redirect σε μια σελίδα η οποία υπόσχεται δωρεάν credit στο Amazon με την μορφή gift card. Το worm αυτό δεν

ενδιαφέρεται για τραπεζικούς λογαριασμούς ή προσωπικά δεδομένα. Στοχεύει όμως σε 2 πράγματα, στα contacts του χρήστη ώστε να στείλει sms μήνυμα σε όσο το δυνατόν περισσότερους χρήστες, και στο συνεχές redirection σε ηλεκτρονικές σελίδες που υποχρεώνει τον χρήστη ώστε να "κερδίσει" την gift card, μαζεύοντας έτσι επισκεψιμότητα σε σελίδες που είναι επικερδείς για τον κακόβουλο χρήστη.

3.1.2. Trojans

Σε αντίθεση με τους ιούς/worms, τα Trojans δεν αυτό-αναπαράγονται μέσα στο περιβάλλον που «μολύνουν». Είναι προγράμματα τα οποία είναι μεταμφιεσμένα ως κάτι που δεν είναι ώστε ο χρήστης να τα εγκαταστήσει στο περιβάλλον εργασίας του. Από εκεί, τα Trojans δρουν δίνοντας προσβάσεις σε τρίτους παίρνοντας έτσι μερικό έλεγχο του υπολογιστή του χρήστη. Αυτό δίνει την δυνατότητα για κλοπή δεδομένων, παρακολούθηση, ενεργοποίηση άλλων υπόγειων ενεργειών κα.

Το GameoverZeus (GoZ) ήταν από τα πιο εξελιγμένα τραπεζικά Trojans καθώς δρούσε σε συνεργασία με άλλες επιθέσεις. Χτύπησε τεράστιο αριθμό τραπεζικών λογαριασμών και ευθύνεται για την απώλεια πολλών εκατομμυρίων λιρών. Το Trojan έφτανε στην μονάδα του χρήστη σαν zip-archive μέσα σε spear-phishing email, τα οποία παρέδιδε το Cutwail Botnet. Εν συνεχεία μπορούν να αντληθούν από την συσκευή πληροφορίες για τραπεζικούς λογαριασμούς ή ακόμα και να γίνει εγκατάσταση επιπλέον malware όπως ransomware ή cryptologgers.

3.1.3. Ransomware

Μια εξαιρετικά ύπουλη μορφή malware, η οποία έχει την ιδιότητα ότι καθιστά απαγορευτική την χρήση του μηχανήματος που έχει μολύνει. Μόλις τεθεί ο περιορισμός, ο επιτιθέμενος, μέσω του προγράμματος απαιτεί λύτρα για την "απελευθέρωση" του σταθμού εργασίας. Το ransomware συνήθως προχωρά σε encryption του δίσκου του τερματικού ή απλά δεν επιτρέπουν σε χρήστη να κάνει Login τερματίζοντας τα δικαιώματα του κάθε λογαριασμού. Το τελευταίο διάστημα έχει απασχολήσει πολύ έντονα τα τμήματα ασφάλειας πληροφοριακών συστημάτων εταιριών καθώς το να καθιστά κάποιος απαγορευτική την χρήση της συσκευής ενός υψηλόβαθμου στελέχους με κρίσιμες πληροφορίες μπορεί να είναι αρκετά προβληματικό. Σε επίπεδο μη εταιρικού χρήστη, όταν η κινητή συσκευή ενός χρήστη αποτελεί, εκτός από τηλέφωνο και φορητό pc, τον τρόπο με τον οποίο πραγματοποιεί πληρωμές, τα ransomware είναι μια απειλή που πρέπει να ληφθεί σοβαρά υπόψη, όχι τόσο για θέμα προστασίας προσωπικών δεδομένων αλλά για θέμα συνέχισης της κανονικής ροής των εργασιών του χρήστη, αυτό που σε μία επιχείρηση θα ονομάζονταν business continuity.

3.1.4. Keyloggers

Σε αντίθεση με τα υπόλοιπα κακόβουλα λογισμικά, ένα keylogger δεν αποτελεί άμεσο κίνδυνο για τον χρήστη και το μηχάνημα του. Όμως, εκμεταλλευόμενο ευπάθειες στο hardware και παράνομο λογισμικό, καταφέρνει και υποκλέπτει εισόδους στο πληκτρολόγιο σε συνδυασμό με screen-shots, λαμβάνοντας έτσι δεδομένα που αφορούν λογαριασμούς μας, όπως ονόματα και κωδικούς χρήστη, αριθμούς τραπεζικών λογαριασμών, στοιχεία επικοινωνίας κα.

Το 2006, οι πελάτες της Σκανδιναβικής τράπεζας Nordea, άρχισαν να λαμβάνουν ένα email, το οποίο φαινόταν να είναι από την τράπεζα, το οποίο τους καλούσε να εγκαταστήσουν στις συσκευές τους ένα anti-spam λογισμικό, το οποίο ήταν επισυναπτόμενο στο μήνυμα. Μόλις το συνημμένο άνοιγε, ξεκίναγε και η μόλυνση του malware γνωστού και ως Haxdoor. Στην αρχή, δεν φαινόταν κάτι ύποπτο, μέχρι που ο χρήστης δοκίμαζε να κάνει Login στην mobile εφαρμογή της τράπεζας. Εκεί, λάμβανε το μήνυμα ότι η σύνδεση απέτυχε και του ζητούσε να ξαναπεράσει τα στοιχεία. Αυτό, ενεργοποιούσε το Keylogger component του malware και αποθήκευε τα στοιχεία που ξαναπέρναγε ο χρήστης, προτού τα στείλει σε κάποιον απομακρυσμένο Server. Πάνω από ένα εκατομμύριο χαθήκαν προτού εντοπιστεί.

3.1.5. Rootkits

Τα rootkits, αποτελούν κακόβουλα προγράμματα τα οποία επιτρέπουν σε τρίτα προγράμματα να δρουν ανενόχλητα σε ένα σταθμό εργασίας καλύπτοντας τις κινήσεις τους από τις βασικές μεθόδους ανίχνευσης. Προσφέρει πρόσβαση στον επιτιθέμενο χωρίς να γίνεται αντιληπτό από τις άμυνες του χρήστη.

Ο Necurs, αποτελεί από τα πιο επικίνδυνα rootkits, καθώς μπορεί να κρύβεται σε επίπεδο root, αποφεύγοντας εντοπισμό εμποδίζοντας ακόμα και την χρήση προγραμμάτων ασφάλειας. Πρόσφατα, εντοπίστηκε να συνεργάζεται με το malware GameoverZeus που αναφέρθηκε παραπάνω, προστατεύοντας malware αρχεία στον δίσκο και στην μνήμη, κάνοντας ακόμα δυσκολότερο τον εντοπισμό και την εξάλειψη του.

3.1.6. Bots

Τα bots είναι μια μορφή malware η οποία μολύνει τερματικά pc, χωρίς όμως απαραίτητα να προκαλούν ζημιά στο τερματικό ή στο λειτουργικό ή ακόμα και στα δεδομένα του χρήστη. Ένα Bot που θα υπάρχει σε ένα pc, κάποια στιγμή θα επικοινωνήσει με μια σειρά από άλλα pc που έχουν το ίδιο bot εγκατεστημένο και θα εκτελέσουν μια προεπιλεγμένη σειρά διαδικασιών. Τέτοιες υλοποιήσεις

malware χρησιμοποιούνται ώστε να προκαλέσουν για παράδειγμα μια μαζική DOS επίθεση σε ένα σύστημα ή να στείλουν μαζικά spam mail μηνύματα, κάνοντας χρήση αρκετών χιλιάδων έως και εκατομμυρίων τερματικών. Το σύνολο των τερματικών που σχηματίζουν αυτό το δίκτυο επίθεσης ονομάζεται Botnet.

Όπως αναφέρθηκε προηγουμένως κατά την περιγραφή του GameoverZeus, το spam botnet Cutwail είναι από τα πιο γνωστά στην κατηγορία τους. Χρησιμοποιεί ένα αυτοματοποιημένο σύστημα βασισμένο σε templates ώστε να δημιουργεί δυναμικά ξεχωριστά emails μαζί με ένα κρυπτογραφημένο πρωτόκολλο επικοινωνίας για να αποφεύγει τα spam filters.

3.1.7. Watering Holes

Είναι η μέθοδος με την οποία δεν μολύνεις απευθείας ένα σύστημα (31). Αντίθετα, η επίθεση πραγματοποιείται σε ένα site το οποίο έχει μεγάλο βαθμό επισκεψιμότητας από τους χρήστες/τερματικά που θέλουμε να επιτεθούμε. Εκμεταλλεύονται συνήθως ευπάθειες τύπου SQL Injection και Cross-site Scripting και οι χρήστες μολύνονται μόλις επισκεφθούν το site. Ως επί το πλείστον, χρησιμοποιούν zero-day ευπάθειες και στοχεύουν sites τα οποία είναι γνωστά και με μεγάλο βαθμό εμπιστοσύνης.

3.2. Jailbreaking and Rooting

3.2.1. Rooting

Ως rooting ορίζεται η διαδικασία κατά την οποία ο χρήστης αποκτά δικαιώματα administrator (root) πάνω στην συσκευή. Αυτό σημαίνει, πως και οι εφαρμογές πλέουν θα εκτελούνται με δικαιώματα administrator, δηλαδή θα έχουν πλήρη πρόσβαση στο σύστημα. Για να γίνει περισσότερο κατανοητό το τι σημαίνει αυτό, αξίζει να αναφερθεί ότι η κάθε εφαρμογή σε Android περιβάλλον εκτελείται με το δικό της User ID (UID), δηλαδή, η κάθε εφαρμογή έχει το δικό της λογαριασμό χρήστη. Κατά συνέπεια, η κάθε εφαρμογή έχει τα δεδομένα της αποθηκευμένα με τρόπο τέτοιο ώστε να μην γίνονται προσβάσιμα από άλλες εφαρμογές. Αυτή η μέθοδος λειτουργίας των εφαρμογών, παύει να ισχύει μόλις η συσκευή γίνει rooted. Η κάθε εφαρμογή πλέον σταματά να λειτουργεί σε sandboxed περιβάλλον και έχει πρόσβαση πλέον σε όλο το σύστημα και κατά συνέπεια σε δεδομένα άλλων εφαρμογών στα οποία η πρόσβαση θα ήταν απαγορευμένη υπό φυσιολογική λειτουργία.

Αυτή η ελευθερία που προσφέρει το rooting δημιουργεί και το πρόβλημα ασφάλειας στις Android συσκευές. Όταν γίνει εγκατάσταση μιας εφαρμογής η οποία έχει μολυνθεί με κάποιο τύπο malware Που αναφέρθηκαν παραπάνω (ή είναι η ίδια κακόβουλη) σε ένα rooted σύστημα, έχει πλέον την

ελευθερία να κινηθεί μέσα στο σύστημα με δικαιώματα root. Οπότε, ένα keylogger θα μπορεί κατά βούληση να αποσπά ονόματα και κωδικούς χρηστών που χρησιμοποιούνται για να γίνει login σε πληθώρα εφαρμογών, όπως για παράδειγμα τραπεζικές mobile εφαρμογές.

3.2.2. Jailbreaking

Κατά αντιστοιχία, το Jailbreaking είναι η διαδικασία κατά την οποία μια συσκευή iOS ο χρήστης αποκτά admin δικαιώματα. Αυτό που γίνεται κατά την jailbreaking διαδικασία είναι ότι στο σύστημα περνάνε ένα παραμετροποιημένο σετ από kernel patches, το οποίο ως αποτέλεσμα έχει να μπορεί στο σύστημα να τρέχει λογισμικό με μη εγκεκριμένο κώδικα και να έχει πρόσβαση σε επίπεδο administrator.

Όπως και με το Rooting, ενώ ο χρήστης αποκτά την δυνατότητα να φέρει ένα iOS σύστημα στα μέτρα του, το Jailbreaking επιτρέπει σε κακόβουλες εφαρμογές να τρέχουν με δικαιώματα administrator πάνω στο σύστημα. Παρόλο που τα φαινόμενα επιθέσεων σε iOS συσκευές είναι πολύ πιο περιορισμένα σε σχέση με τις Android συσκευές, οι κίνδυνοι παραμένουν οι ίδιοι.

3.3. Εφαρμογές Υπηρεσίας (Native Apps)

Ο όρος αυτός χρησιμοποιήται για να περιγράψει εφαρμογές οι οποίες προσφέρονται από εταιρίες για έναν συγκεκριμένο σκοπό (32). Για τους σκοπούς της εργασίας θα περιοριστεί σε εφαρμογές πληρωμών που δύναται να έχει ο κάθε έμπορος για κινητές συσκευές χωρίς πλέον να υπάρχει η ανάγκη να γίνει η online αγορά μέσα από web-browser. Σίγουρα υπάρχουν κίνδυνοι γενικότερα στον χώρο των Online αγορών, αλλά οι ευπάθειες των browsers είναι κοινές και γίνονται άμεσα γνωστές οπότε και αντιμετωπίζονται αποτελεσματικότερα και σε μαζικό επίπεδο (με μία αναβάθμιση). Στο σενάριο των επιμέρους εφαρμογών ανά έμπορο/εταιρία, θα πρέπει να υπάρχει ανάλυση ρίσκου και αντιμετώπισης του για την κάθε μια ξεχωριστά όπως επίσης και την ξεχωριστή υλοποίηση της ανά πλατφόρμα (Android, iOS κα). Αρκετές από τις εταιρίες δεν έχουν τις γνώσεις και τους πόρους να προχωρήσουν σε ασφαλείς λύσεις όπως για παράδειγμα ανάλυση συμπεριφοράς (behavior/pattern analysis) και καταλήγουν σε σενάρια one-factor authentication (απλό username και password).

3.4. Μεθοδολογίες-Τεχνολογίες Πληρωμών

Οι αγορές μέσω κινητών συσκευών στηρίζονται σε ήδη παγιωμένα συστήματα online πληρωμών. Αυτό σημαίνει πως ότι γηγενείς αδυναμίες έχει το υπάρχον σύστημα απειλεί και τις Mobile πληρωμές, όπως για παράδειγμα προβλήματα που σχετίζονται με τις POS συσκευές, αλλά και επιπλέον οι

ευπάθειες των κινητών συσκευών αποτελούν κινδύνους για τις εγχρήματες συναλλαγές, όπως για παράδειγμα τα malware που μαστίζουν τα κινητά που αναφέρθηκε προηγουμένως.

Το NFC δεν παρείχε native δυνατότητες κρυπτογράφησης. Το RFID επιτρέπει την ανάγνωση σε παθητική υλοποίηση μέχρι και 10 μέτρα, που σημαίνει ότι το σήμα μπορεί να υποκλαπεί από απόσταση και η επικοινωνία είναι one-way. Και στις δύο περιπτώσεις απαιτείται κρυπτογράφηση και μέθοδοι όπως tokenization. Τα κλειδιά που χρησιμοποιούνται αντίστοιχα, δεν θα πρέπει σε καμία περίπτωση να είναι μίας χρήσης και να μην είναι κοινά για όλους τους λογαριασμούς. Τα secure elements που βρίσκονται στις SIM κάρτες ή σε ανεξάρτητο chip στις συσκευές, αποτελούν επίσης σημείο ρίσκου κατά την παραγωγή τους αλλά και την ενσωμάτωση τους στην συσκευή ανάλογα την υλοποίηση (33).

Πέρα από τα αυστηρά τεχνολογικά θέματα, σημαντικό ρόλο παίζουν και οι οντότητες που στο σύνολο τους σχηματίζουν το (τραπεζικό) σύστημα πληρωμών. Ποιος θα είναι (αν θα έχει) ο ρόλος των τραπεζών (Issuer, Acquirer), του merchant, των πάροχων συσκευών και γραμμών επικοινωνίας κα. η εισαγωγή της έννοιας token και TSP, σήμαινε ότι κάποια οντότητα θα αναλάμβανε και αυτό τον ρόλο ή θα υπήρχε η απαίτηση να φτιαχτεί μία οντότητα αυτόνομη η οποία να εκπληρώνει τον ρόλο αυτό.

4. Ενναλακτικές Υλοποιήσεις-Ενώνοντας Παρελθόν με το Παρόν

Για να γίνει περισσότερο κατανοητή το πώς εξελίχθηκαν τα mobile wallets και τα συστήματα πληρωμής στην σημερινή τους μορφή , θα ήταν χρήσιμο να γίνει μία συνοπτική αναφορά σε παλαιότερες υλοποιήσεις, οι οποίες είτε τερματίστηκαν είτε υπάρχουν ακόμα και εξυπηρετούν συγκεκριμένες πληθυσμιακές ομάδες. Οι υλοποιήσεις αυτές αφορούν τόσο mobile wallets αλλά και εναλλακτικές μορφές συστημάτων πληρωμής.

4.1. Προπληρωμένος Χρόνος Ομιλίας ως Νόμισμα

Ένα ευρέος διαδεδομένο σύστημα πληρωμών, ειδικά σε περιοχές της Αφρικής και της Ασίας είναι η χρήση προπληρωμένου χρόνου ομιλίας ως νόμισμα (34). Οι MNO αντιλήφθηκαν ότι υπάρχει μεγάλη ανάγκη για μεταφορά εμβασμάτων ειδικά σε περιοχές όπου δεν υπήρχαν πολλά καταστήματα τραπεζών ή περιοχές όπου απλά δεν κυκλοφορούν μετρητά. Οπότε, ξεκίνησε να γίνεται αγορά μεταφορά χρόνου ομιλίας από συνδρομητή τηλεφωνικής υπηρεσίας σε κάποιον άλλο συνδρομητή P2P. Τον χρόνο τον αγόραζαν από κάποιον retailer ο οποίος με την σειρά του τον αγόραζε από το αντίστοιχο MNO δίκτυο. Ο χρόνος αυτός μπορούσε να εξαργυρωθεί ύστερα σε μετρητά. Η μέθοδος αυτή ενώ ξεκίνησε για μεταφορές χρημάτων P2P, εξελίχθηκε και σε πληρωμές αγαθών. Χαρακτηριστικό είναι το παράδειγμα η Ζιμπάμπουε, όπου σύμφωνα με το Εθνικό Παράρτημα Εμπορίου “οι πελάτες είχαν κουραστεί να δέχονται ως ρέστα για μικροποσά σοκολάτες, καθώς το Αμερικάνικο Δολάριο δεν είχε μεγάλη ροή στην αγορά (35)”.

Ο προ-πληρωμένος χρόνος ομιλίας ως νόμισμα έχει πολύ δυνατή παρουσία σε χώρες όπως Αίγυπτος, Ουγκάντα Κένυα και γενικά σε περιοχές της Αφρικής όπου οι τραπεζικές υπηρεσίες και παρουσία ήταν ελλιπής όπως στην Νότια Αφρική και στις Φιλιππίνες. Αλλά και στις ΗΠΑ έχουν γίνει πιλοτικά προγράμματα για υπηρεσίες χρέωσης απευθείας του λογαριασμού της κινητής τηλεφωνίας για αγορές αγαθών με μικροποσά.

Οι κυρίαρχες τεχνολογίες που χρησιμοποιήθηκαν ήταν τα SMS μηνύματα και το πρωτόκολλο WAP. Εμφανίστηκαν επίσης και εφαρμογές για τα κινητά που επέτρεπαν P2P μεταφορές. Πάντως, η μέθοδος με SMS φάνηκε να παγιώνεται ως υλοποίηση λόγω της απλότητας και της διαλειτουργικότητας της ανεξαρτήτου συσκευής. Πάντως, σε πληρωμές σε καταστήματα δεν είχε πολύ μεγάλη αποδοχή λόγω της χαμηλής ποιότητας στην ασφάλεια που

παρείχε, καθώς το κείμενο του SMS μηνύματος, ήταν σε plaintext μορφή κατά την μεταφορά του (36).

Μία από τις πλέον αξιόλογες και πρωτοπόρες εταιρίες που εκμεταλλεύτηκαν αυτή τη δομή, ήταν η M-PESA. Με έδρα, αρχικά την Κένυα, ιδρύθηκε το 2007 από την Vodafone για λογαριασμό της Safaricom και Vodacom που είναι οι 2 μεγαλύτεροι MNOs της Κένυας. Αρχικά ξεκίνησε με την προοπτική να προσφέρει καλύτερη διαχείριση στη μεταφορά και αποπληρωμή δανείων και ίσως και στην επίτευξη καλύτερων τόκων λόγω μικρότερου κόστους των συναλλαγών. Τώρα πλέον υποστηρίζει κατάθεση χρημάτων (37), αποστολή χρημάτων σε αριθμό κινητού τηλεφώνου, πληρωμές λογαριασμών, πληρωμές σε εμπόρους κα και όλα αυτά χωρίς την παρουσία των τραπεζών, οπότε οι οντότητες Issuer και Acquirer δεν έχουν ρόλο σε αυτή την αρχιτεκτονική. Για να υπάρχει όμως μία σύμπλευση με τα διεθνή πρότυπα ασφάλειας και τις τάσεις της αγοράς σε θέματα βέλτιστων πρακτικών, η M-PESA υιοθέτησε τα KYC (Know Your Customer) προ-απαιτούμενα για τον υποψήφιο χρήστη της υπηρεσίας. Έτσι συγκεντρώνονται κάποια ελάχιστα στοιχεία και έγγραφα για τον πελάτη, τα οποία ελέγχονται και από την τράπεζα (για παράδειγμα, μια ταυτότητα). Οι εφαρμογές της M-PESA είναι εγκατεστημένες ,μέσα στην SIM κάρτα της συσκευής, η οποία κάρτα διαχειρίζεται και την αυθεντικοποίηση.

4.2. Πληρωμή μέσω Λογαριασμού κινητής Τηλεφωνίας

Στην άλλη πλευρά του Ατλαντικού, η εταιρία Boku, προσφέρει μια διαφορετική προσέγγιση στις online πληρωμές, χωρίς την μεσολάβηση τραπεζών ή την χρήση χρεωστικών/πιστωτικών καρτών. Η λύση που προσφέρει η εταιρία είναι αρκετά πρωτοποριακή και δίνει την δυνατότητα για την απευθείας χρέωση του λογαριασμού του κινητού τηλεφώνου για τις αγορές. Ξεκίνησε προσφέροντας δυνατότητα αγοράς virtual αγαθών, για παράδειγμα στην κοινότητα των online video-games, έχοντας συνεργασία με εταιρίες όπως Electronic Arts, IGG, Playfish και Games-Master, αλλά επεκτάθηκε τόσο σε online merchants όσο και σε Brick & store καταστήματα. Επιτρέπει την χρέωση τόσο online όσο και offline από κινητό, desktop pc, παιχνιδομηχανή ακόμα και Smart-TV. Δημιουργήθηκε το 2008 με έδρα το San Francisco, έχει κάνει μια υψηλού προφίλ συνεργασία με την Deutsche Telekom ανοίγοντας γραφεία στην Ευρώπη, Ασία και Λατινική Αμερική, ενώ παράλληλα είχαν προτάσεις εξαγοράς τόσο από την Apple όσο και την Google (38).

Ένας έμπορος μπορεί με μια απλή αίτηση να δηλώσει να συμμετέχει της Boku συμπληρώνοντας απλά μια Online φόρμα. Ένας πελάτης μπορεί να δηλώσει και να αποθηκεύσει τον τηλεφωνικό του αριθμό σε έναν Merchant ο οποίος συνεργάζεται με την Boku ώστε να μην χρειάζεται κάθε φορά να δηλώνει το νούμερο του στην φόρμα αγοράς για τον συγκεκριμένο Merchant. Η εξουσιοδότηση αυτή διαρκεί για 90 ημέρες ή για ένα συνολικό ποσό αγορών της τάξης των 100 δολαρίων, για θέμα ασφάλειας. Η εταιρία είναι συμμορφωμένη σε θέματα διαφάνειας, απόδοσης ευθυνών και προσωπικών δεδομένων με το πρότυπο της TRUSTe η οποία ειδικεύεται ως 3rd party στην επίτευξη Online trust ανάμεσα σε υπηρεσίες και καταναλωτές.

5. Apple Pay

5.1. Εισαγωγή

Τον Οκτώβριο του 2014, η Apple κυκλοφόρησε την εφαρμογή που θα αναζωπύρωνε το χαμένο ενδιαφέρον για τις εγχρήματες συναλλαγές μέσω πλατφόρμας κινητού τηλεφώνου (και όχι μόνο), ξεπερνώντας κατά πολύ εταιρίες που προσπάθησαν ήδη (Google, Softcard-former ISIS).

Η εφαρμογή είναι συμβατή σε λειτουργικό σύστημα iOS 8.1 ή νεότερο, και αρχικά ήταν διαθέσιμη για συσκευές τηλεφώνου iPhone 6 και μεταγενέστερες, Apple Watch αλλά και σε ορισμένα μοντέλα tablet. Αργότερα, έγινε εφικτή η χρήση του και στις παλαιότερες συσκευές iPhone 5 μέσω σύζευξης τους με το Apple Watch. Η χρήση του επιτρέπεται τόσο σε POS τερματικά όσο και σε Online αγορές με εξαίρεση την χρήση της εφαρμογής σε Tabs τα οποία περιορίζονται μόνο σε Online συναλλαγές (και όχι σε POS).

Το καταναλωτικό κοινό υποδέχθηκε την υπηρεσία με μεγάλο ενθουσιασμό καθώς τις τρεις πρώτες ημέρες δηλώθηκαν πάνω από ένα εκατομμύριο κάρτες στην εφαρμογή και τουλάχιστον 200 χιλιάδες vendors δήλωσαν ότι θα προχωρήσουν στην υποστήριξη της. Αυτή την στιγμή ο Καναδάς και η Αυστραλία το στηρίζουν μέσω της American Express, η Βρετανία, η 1η Ευρωπαϊκή χώρα στην οποία παρουσιάστηκε το στηρίζει με 15 τράπεζες να δέχονται συναλλαγές με τις κάρτες τους, ενώ στην Αμερική όπου και ξεκίνησε έχει την υποστήριξη 786 (και αυξάνονται) τραπεζών (39). Από το Φεβρουάριο του 2016, είναι πολύ πιθανό να κάνει την εμφάνιση της και στην Κίνα, ύστερα από ένα προ-συμφωνητικό που έχει υπογραφεί με την Κινέζικη Union Pay Co.

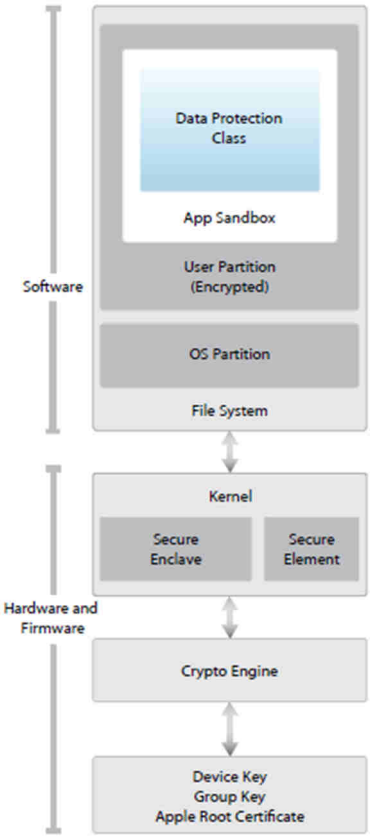
Τα θεμέλια της ιδέας είχαν δημιουργηθεί πολλά χρόνια πριν, και για την υλοποίηση της η Apple συνεργάστηκε με τις American Express, MasterCard και Visa σε μια κοινή προσπάθεια να βρεθεί λύση να έχουμε συναλλαγές χωρίς να απαιτείται η αποστολή προσωπικών πληροφοριών από πλευράς του χρήστη.

Ο τύπος της άδειας της εφαρμογής είναι ιδιοκτησιακός (proprietary), που σημαίνει ότι έχει κατηγοριοποιηθεί ως μη-δωρεάν πρόγραμμα, κλειστού κώδικα. Κατά συνέπεια, η Apple διατηρεί αρκετά δικαιώματα πάνω στο προϊόν της όπως για παράδειγμα περιορισμό στην χρήση του, μεταβολή και έλεγχο του κώδικα κα.

5.2. Λειτουργία Apple Pay

5.2.1. Δομικά στοιχεία της αρχιτεκτονικής του Apple Pay

Στην αρχιτεκτονική του iOS, όπως φαίνεται στο σχήμα **(εικόνα_18),** είναι ορατά τα πιο σημαντικά τμήματα της που αφορούν το Apple Pay (40).



Εικόνα 18 Αρχιτεκτονική Ασφάλειας iOS 9, By Apple-iOS Security Guide

- **Secure Element**: είναι το chip πάνω στο οποίο τρέχει η πλατφόρμα της Java Card. Αξίζει να αναφερθεί ότι Java Card είναι η μικρότερη μέχρι τώρα πλατφόρμα της Java η οποία έχει αναπτυχθεί για συσκευές με embedded (πολύ συγκεκριμένη) λειτουργία και συναντάται κατά κόρον σε κάρτες SIM και ATM. Όταν μια κάρτα γίνεται δεκτή για χρήση με το Apple Pay, ο TSP στέλνει στη συσκευή ένα token (η Apple το ονομάζει DAN) το οποίο θα αντικαταστήσει μόνο τον πραγματικό αριθμό PAN της κάρτας, και θα βρίσκεται αποθηκευμένος στο SE.

- **Ελεγκτής NFC**: είναι υπεύθυνος για την αναμετάδοση δεδομένων ανάμεσα στον επεξεργαστή εφαρμογής (application processor) και το Secure Element, και ανάμεσα στο Secure Element και την μονάδα POS.
- **Wallet**: ή πρώην Passbook, αναφέρεται στην εφαρμογή της Apple η οποία είναι υπεύθυνη για την διαχείριση των καρτών (πιστωτικών, debit, δώρων) που υπάρχουν στον λογαριασμό του χρήστη. Επιτρέπει τον έλεγχο πληροφοριών αναφορικά με τις κάρτες όπως τελευταίες συναλλαγές αλλά και την προσθήκη καρτών προς χρήση για το Apple Pay.
- **Secure Enclave**: εδώ είναι μία από τις πλέον ουσιαστικές υπερβάσεις της Apple στο θέμα της ασφάλειας. Το στοιχείο αυτό είναι ένας συν-επεξεργαστής τοποθετημένος μαζί με τους A7 επεξεργαστές της Apple (και μεταγενέστερα μοντέλα). Είναι απομονωμένος από τον υπόλοιπο επεξεργαστή και το iOS, και έρχεται με μία ενσωματωμένη γεννήτρια τυχαίων αριθμών βασισμένη σε πολλαπλούς ring oscillators και κατόπιν σε επεξεργασία μέσω μηχανής CTR_DRBG. Από κατασκευής, έχει ένα μοναδικό αριθμό το UID (Unique ID), ένα AES 256 bit κλειδί αποτυπωμένο πάνω στο τσιπ, το οποίο όπως θα φανεί παρακάτω έχει πολύ σημαντικό ρόλο στο κομμάτι του Apple Pay, και δεν το «κοινοποιεί» σε κανένα άλλο κομμάτι της συσκευής. Κάθε φορά που η συσκευή κάνει start-up, δημιουργείται ένα τυχαίο κλειδί το οποίο σε συνδυασμό με το UID χρησιμοποιούνται για να κρυπτογραφήσουν το τμήμα της μνήμη της συσκευής που χρησιμοποιείται από το Secure Enclave. Διαθέτει δικό του secure boot και customized software update διαφορετικό από αυτό του application επεξεργαστή.

  Η λειτουργικότητα που διαθέτει και εξετάζεται στο πλαίσιο της παρούσας εργασίας, είναι η δυνατότητα του συγκρίνει τα δεδομένα από το δακτυλικό μας αποτύπωμα σε σχέση με το μαθηματικό «κλειδί» που έχει αποθηκευτεί από την αρχική μας δήλωση του αποτυπώματος και αναλόγως να επιτρέπει ή να απαγορεύει την πρόσβαση στη συσκευή Apple.

  Ουσιαστικά, είναι ο μηχανισμός αυθεντικοποίησης του χρήστη κάνοντας χρήση των αποθηκεμένων δεδομένων του Touch ID.

Όταν ο cardholder προσπαθεί να ξεκλειδώσει την συσκευή του με το δακτυλικό αποτύπωμα, η επικοινωνία ανάμεσα στον δέκτη του Touch ID και στον επεξεργαστή της συσκευής γίνεται μέσω ενός SPI διαύλου (serial peripheral interface). Ο επεξεργαστής της

συσκευής με την σειρά του προωθεί τα δεδομένα του αποτυπώματος στο Secure Enclave αλλά δεν είναι σε θέση να τα διαβάσει καθώς η πληροφορία είναι κρυπτογραφημένη και αυθεντικοποιημένη.

Αυτό επιτυγχάνεται με χρήση ενός session κλειδιού το οποίο δημιουργείται από το **shared pairing κλειδί** που παρέχεται για τον αισθητήρα του Touch ID και του Secure Enclave. Η δημιουργία του κλειδιού γίνεται μέσα στο Secure Enclave από το Unique ID κλειδί του και το UID του secure Element. Αυτό με την σειρά του μεταφέρεται από το Secure Enclave σε ένα HSM module, τα οποία είναι συσκευές που χρησιμοποιούνται για φύλαξη και διαχείριση ψηφιακών κλειδιών και λειτουργούν με πρότυπα όπως Common Criteria και FIPS 140 (41), και αφού το επεξεργαστεί το περνάει στο Secure Element. Η ανταλλαγή των session κλειδιών γίνεται με την χρήση AES key wrapping, δηλαδή τα κλειδιά κρυπτογραφούνται σπάζοντας σε n κομμάτια των 64 bit το καθένα (42), οπότε η κάθε μεριά παρέχει από ένα τυχαίο κλειδί για τις ανάγκες του session και μεταφέρονται χρησιμοποιώντας ένα CCM mode του AES, παρέχοντας έτσι και counter μέσω του initialization vector

- **Apple Pay servers**: είναι υπεύθυνοι για την διαχείριση των καρτών που έχουν δηλωθεί στην εφαρμογή Wallet και των αριθμών λογαριασμού που βρίσκονται στο Secure Element.
- **Touch ID:** είναι το βιομετρικό σύστημα το οποίο ανιχνεύει το δακτυλικό αποτύπωμα του χρήστη και επιτρέπει την ασφαλή προσπέλαση στην συσκευή. Το κουμπί είναι φτιαγμένο από κρύσταλλο ζαφείρι, το 3ο πιο σκληρό υλικό στην κατηγορία των ορυκτών. Διαβάζει το αποτύπωμα από κάθε γωνία υποδερμικά μέσω του μεταλλικού δακτυλιδιού, χρησιμοποιώντας capacitive touch τεχνολογία (αντιλαμβάνεται ηλεκτρικούς παλμούς) λαμβάνοντας υπόψη λεπτομέρειες που δεν είναι ορατές με γυμνό μάτι όπως πόρους, καμπύλες κα δημιουργώντας μια αρχική raster εικόνα η οποία αποτυπώνεται προσωρινά στο Secure Enclave. Εν συνεχεία, δημιουργεί μια μαθηματική αντιπροσώπευση του αποτυπώματος με διανύσματα, η οποία δεν διαθέτει καμία πληροφορία για την ταυτότητα του χρήστη και την οποία κρατά κρυπτογραφημένη στο Secure Enclave. Η διαδικασία του «κτισίματος» του αποτυπώματος συνεχίζετε με κάθε χρήση του προσθέτοντας περισσότερα στοιχεία. Η χρήση κωδικού εισόδου δεν απαιτείται πλέον αν και υπάρχουν ακόμα συνθήκες που απαιτούν την χρήση του ως έξτρα μέτρο ασφάλειας, όπως
    - Η συσκευή μόλις άνοιξε
    - Η συσκευή δεν έχει χρειαστεί να ξεκλειδωθεί για πάνω από 48 ώρες

- Έγιναν 5 αποτυχημένες απόπειρες ξεκλειδώματος με την χρήση δακτυλικού αποτυπώματος
- Όταν ορίζεται στην συσκευή νέο δακτυλικό αποτύπωμα

Η λειτουργία του όμως που αφορά αυτή την έρευνα, είναι ο ρόλος του στις συναλλαγές μέσω Apple Pay.

5.2.2. Δήλωση καρτών για χρήση με το Apple Pay

5.2.2.1. Εισαγωγή

Όταν ο cardholder προσθέτει μια κάρτα (credit ή debit) στο Apple Pay, η Apple στέλνει με **ασφάλεια** τα στοιχεία της κάρτας, μαζί με κάποια επιπλέον στοιχεία του κατόχου και της συσκευής, στην εκδότρια αρχή. Ελέγχοντας τις πληροφορίες αυτές, ο φορέας της κάρτας θα αποφασίσει την προσθήκη ή όχι της κάρτας στο Apple Pay.

Για την αποστολή των πληροφοριών προς επικύρωση της κάρτας, η Apple χρησιμοποιεί τρεις server-side κλήσεις που στο σύνολο τους αποτελούν το αίτημα του χρήστη για την προσθήκη της κάρτας στο Apple Pay και είναι τα α. πεδία πληροφοριών (check fields), β. έλεγχο της κάρτας και γ. δρομολόγηση και παροχή της κάρτας στην υπηρεσία (Link & provision).

Αντίστοιχα, ο Issuer, χρησιμοποιεί και απαντά σε αυτές τις κλήσεις για να α. επαληθεύσει τα στοιχεία τη κάρτας, β. δώσει την έγκριση του και γ. προσθέσει την κάρτα στο Apple Pay.

Και τα τρία αυτά sessions γίνονται με κρυπτογράφηση SSL.

Ποτέ ο αριθμός μιας κάρτας δεν είναι αποθηκευμένος στην συσκευή ή στους servers της Apple. Αυτό που χρησιμοποιείται είναι το **DAN** (device account number) το οποίο δημιουργείται, κρυπτογραφείται και αποθηκεύεται στο **Secure Element** της κάρτας και είναι μοναδικός ανά κάρτα και συσκευή. Ο αριθμός αυτός είναι τελείως διαφορετικός από τους αριθμούς των καρτών στην δομή του, η κρυπτογράφηση του είναι τέτοια που η Apple δεν μπορεί να τον δει, δεν έχει καμία επικοινωνία με το υπόλοιπο iOS λόγω της θέση του στο Secure Element και δεν γίνεται Back up στο iCloud.

Υπάρχουν δύο τρόποι να προστεθεί μια κάρτα στο Apple Pay, είτε η κάρτα υπάρχει ήδη στον λογαριασμό στο iTunes, είτε προσθήκη καινούργιας κάρτας.

5.2.2.2. Προσθήκη καινούργιας κάρτας

Για την προσθήκη της κάρτας «με το χέρι» μέσα από τις ρυθμίσεις τις συσκευής και την εφαρμογή Wallet, εισάγονται οι απαραίτητες πληροφορίες (όνομα, αριθμός κάρτας, ημερομηνία λήξης και CVV) ή εναλλακτικά χρησιμοποιήται η iSight κάμερα της συσκευής για να τραβηχτεί φωτογραφία της κάρτας. Η φωτογραφία αυτή ΔΕΝ αποθηκεύεται ποτέ στην συσκευή ή στο φωτογραφικό άλμπουμ. Μόλις συμπληρωθούν όλα τα απαραίτητα πεδία, το process Check Card προχωρά στην επιβεβαίωση όλων των πεδίων εκτός του CVV, τα κρυπτογραφεί και τα στέλνει στους Apple Pay servers χρησιμοποιώντας το 2^{ο} από τα τρία sessions (κλήσεις) που αναφέρθηκαν παραπάνω.

Εάν στο process Check Card επιστραφεί ένα id που περιέχει τους όρους και συνθήκες χρήσης από τον φορέα της κάρτας, τότε η Apple κατεβάζει και φέρνει στην οθόνη του χρήστη τους όρους αυτούς. Εφόσον ο cardholder δεχθεί τους όρους τότε και μόνο τότε η Apple προωθεί το CVV της κάρτας μαζί με ένα id το οποίο υποδηλώνει ότι οι όροι χρήσης έγιναν δεκτοί, προς το 3^{ο} session (κλήση) δρομολόγηση και παροχή. Στην διάρκεια αυτού του session, η Apple μοιράζεται πληροφορίες με τον πάροχο της κάρτας όπως αριθμό τηλεφώνου, τύπος συσκευής, περιοχή και ώρα που γίνεται η διαδικασία (εάν η κάρτα έχει εκδοθεί στην Ελλάδα και η εντολή για προσθήκη στο Apple Pay γίνει από πχ στην Βραζιλία, αυτό κινεί υποψίες), κινήσεις λογαριασμού μέσω του iTunes και App Store(behavior analysis το οποίο αποτελεί dynamic data σε αντίθεση με κάτι «σταθερό» όπως SSN-social security number), ώστε ο πάροχος να κρίνει εάν η κάρτα θα προστεθεί στο Apple Pay.

Στο τέλος του 3^{ου} session, ο Issuer προωθεί το PAN της κάρτας στον TSP για να δημιουργήσει το token (DAN) που θα αντιστοιχεί σε αυτή την κάρτα. Το token το παραλαμβάνει ο TSM της Apple και το προωθεί για αποθήκευση στο SE της συσκευής. Επιπλέον, η συσκευή ξεκινά να κατεβάζει στο Wallet το αρχείο Pass που θα είναι η κωδικοποιημένη μορφή της κάρτας, και παράλληλα γίνεται και η διασύνδεση της κάρτας με το secure element.

Το αρχείο Pass περιέχει διάφορα URLs ώστε να κατέβουν διάφορα δεδομένα που αφορούν την κάρτα όπως εικόνες art της κάρτας, metadata, την εφαρμογή του παρόχου κτλ. Επιπλέον περιέχει πληροφορίες όπως εάν η κάρτα είναι ενεργή ή όχι, logs αναφορικά με το αν

ολοκληρώθηκε η διαδικασία σύνδεσης της κάρτας με το secure element, εάν χρειάζονται επιπλέον στοιχεία για χρήση της κάρτας για πληρωμές κα.

Κάθε κάρτα μπορεί να προστεθεί μέχρι και σε δέκα συσκευές. Η δήλωση της πρέπει να γίνει σε κάθε συσκευή ξεχωριστά.

5.2.2.3. Προσθήκη κάρτας μέσα από το iTunes

Για να γίνει προσθήκη της κάρτας στο Apple Pay Μέσα από το iTunes, ο cardholder θα χρειαστεί να εισάγει ξανά τον κωδικό του για το Apple ID. Τα στοιχεία της κάρτας είναι ήδη περασμένα οπότε με το 2ο session (Check Card) γίνεται αποστολή των στοιχείων. Όπως και πριν, εάν η κάρτα εγκριθεί για χρήση μέσω Apple Pay, πληροφορίες για τους όρους χρήσης κατεβαίνουν στην συσκευή και μόλις γίνουν αποδεκτοί, στέλνετε η αποδοχή και το CVV της κάρτας μέσω του 3ου session call.

5.2.2.4. Προσθήκη Κάρτας μέσω εφαρμογής του Φορέα της Κάρτας

Για να προστεθεί κάρτα στο Apple Pay μέσω εφαρμογής ενός φορέα Καρτών, θα πρέπει αυτή η εφαρμογή να είναι πιστοποιημένη για χρήση με το Apple Pay (ακούγεται αυτονόητο, αλλά δεν είναι, μπορεί η εφαρμογή να είναι από 3rd party provider). Εάν είναι πιστοποιημένη για χρήση, η διαδικασία προσθήκης της κάρτας είναι ίδια με το να προσθέταμε manually μια κάρτα, με τη μόνη σημαντική διαφορά ότι αντί για το CVV, το στοιχείο που ανταλλάσσεται κατά το 3ο session call είναι ένα one-time password.

5.2.2.5. Επιπλέον επαλήθευση των στοιχείων

Υπάρχει πάντα το ενδεχόμενο ανάλογα της εκδότριας αρχής της κάρτας, να ζητηθεί ένα επιπλέον βήμα πιστοποίησης του χρήστη. Αυτό μπορεί να είναι μήνυμα, email, τηλέφωνο στην υπηρεσία εξυπηρέτησης ή μέσω εφαρμογής κάποιου third party παρόχου που θα ολοκληρώσει την επαλήθευση, ακόμα και να κάνει log-in στον λογαριασμό τους στην δικτυακή πλατφόρμα της εκδότριας τράπεζας. Στην περίπτωση του μηνύματος ή email, θα σταλθεί στον χρήστη ένας κωδικός τον οποίο θα πρέπει να εισάγει στα settings του Wallet app. Για την περίπτωση όπου η επιβεβαίωση γίνει μέσω κάποιας υπηρεσίας εξυπηρέτησης πελατών ή μιας 3rd party οντότητας, την επικοινωνία θα πρέπει να την κάνει ο cardholder.

5.2.2.6. *Αφαίρεση-Διαγραφή-Αναστολή κάρτας*

Ο cardholder, έχει την δυνατότητα να παγώσει την λειτουργία του Apple Pay στις συσκευές του εάν τις δηλώσει σε Lost Mode μέσω της υπηρεσίας Find my iPhone που του επιτρέπει να κλειδώσει την συσκευή του, να προχωρήσει σε Remote Wipe της συσκευής, ή απλά να αφαιρέσει επιλεκτικά κάρτες από το Wallet του. Οι φορείς της κάρτας ή το αντίστοιχο Payment network ενημερώνεται για την διαγραφή των καρτών ακόμα και εάν το κινητό είναι εκτός δικτύου. Εάν για τον οποιοδήποτε λόγω ο cardholder έχει αμφιβολίες για το κατά πόσο η κάρτα/κάρτες του έχουν αφαιρεθεί επιτυχώς από το Wallet και δεν γίνονται δεκτές από το Apple Pay, μπορεί να επικοινωνήσει απευθείας με τον φορέα της κάρτας.

Εάν κριθεί απαραίτητο η επιλογή μιας πιο ακραίας λύσης, να γυρίσει η συσκευή στα factory defaults, μέσα από το "Find my iPhone" όπως αναφέρθηκε παραπάνω, το iOS δίνει εντολή στο Secure Element να θεωρήσει όλες της κάρτες ως διαγραμμένες. Αυτόματα, είναι αδύνατο να πραγματοποιηθεί συναλλαγή στο Apple Pay. Παράλληλα, το Secure Enclave ακυρώνει και όλα τα AR (δες "**Διαδικασία πληρωμής μέσω Apple Pay**", παρακάτω) των καρτών που έχει αποθηκευμένα. Έτσι, ακόμα και αν μια συναλλαγή έχει ξεκινήσει, θα ακυρωθεί. Μόλις η συσκευή μπει online, προσπαθεί άμεσα να επικοινωνήσει με τους Servers της Apple ώστε να βεβαιωθεί ότι θα ακυρωθούν οι κάρτες που είναι στο Secure Element.

5.2.3. Διαδικασία πληρωμής μέσω Apple Pay

5.2.3.1. Εξουσιοδότηση πληρωμής

Όταν ο cardholder της υπηρεσίας βρεθεί μπροστά από τερματικό POS το οποίο έχει το σήμα που το ξεχωρίζει ως NFC ready, μπορεί να ξεκινήσει μια contactless συναλλαγή. Το P.O.S τερματικό επικοινωνεί απευθείας με το secure Element μέσω του NFC controller διαμέσου ενός δίαυλου ο οποίος έχει αποκλειστικά αυτή τη λειτουργία.

Την επιβεβαίωση για να επιτρέψει το Secure Element να προχωρήσει η πληρωμή, θα έρθει από το Secure Enclave, το οποίο θα δηλώσει κατά πόσο ο cardholder αυθεντικοποιήθηκε μέσω του Touch ID ή του Passcode. Το Touch ID είναι η default επιλογή εκτός εάν γίνουν 3 ανεπιτυχής προσπάθειες μέσω δακτυλικού αποτυπώματος ή εάν το touch ID δεν έχει παραμετροποιηθεί προς χρήση.

Η επικοινωνία ανάμεσα στο Secure Enclave και το Secure Element γίνεται μέσω ενός σειριακού προτύπου, όπου το Secure Element συνδέεται με τον NFC controller και αυτός με την

σειρά του με τον application processor. Η επικοινωνία του Enclave με το Element γίνεται με την χρήση του shared pairing κλειδιού (κλειδί που είναι κοινό και για τις 2 οντότητες και η επικοινωνία γίνεται πάνω σε κοινό κανάλι).

Μόλις το Secure Enclave επιβεβαιώσει το δακτυλικό αποτύπωμα του χρήστη, στέλνει signed δεδομένα στο Secure Element σχετικά με τον τύπο της αυθεντικοποίησης που έγινε (επιτυχής /ανεπιτυχής, τι αφορά) και πληροφορίες σχετικά με τον τύπο της συναλλαγής (μέσω NFC, μέσω εφαρμογής). Τα δεδομένα αυτά εκτός signed, συνοδεύονται και από ένα επιπλέον μέγεθος που ονομάζεται Authorization Random (AR).Το AR δημιουργείται εντός του Secure Enclave όταν γίνεται 1η φορά η καταχώρηση μια κάρτας. Είναι μοναδικό ανά κάρτα (αλλά όχι σταθερό, θα δοθούν διευκρινήσεις παρακάτω). Παραδίδεται στο Secure Element μαζί με την βεβαίωση της αυθεντικοποίησης του χρήστη μέσω του pairing key, με ην ίδια μέθοδο που περιεγράφηκε παραπάνω, οπότε είναι κρυπτογραφημένο και προστατευμένο από replay attacks.

Μόλις λοιπόν, το Secure Element λάβει το πακέτο αυθεντικοποίησης από το Secure Enclave, επιτρέπει να προχωρήσει η εφαρμογή για την συναλλαγή μέσω είτε NFC-enabled POS είτε εφαρμογές που έχουν οι Merchants.

Το AR όπως αναφέρθηκε παραπάνω, δεν είναι σταθερό. Είναι μεν μοναδικό για κάθε κάρτα, αλλά για λόγους ασφάλειας υπάρχουν συνθήκες που δημιουργείται καινούργιο. Όταν δημιουργείται καινούργιο, το παλιό AR απενεργοποιείται και δεν γίνεται δεκτό από το Secure Enclave. Μερικοί από τους λόγους που γίνεται αυτό είναι,

- Το Passcode γίνεται disabled
- Ο Cardholder κάνει log out από το iCloud
- Γίνεται restore της συσκευής από το Recovery Mode
- Γίνεται διαγραφή όλων των περιεχομένων και ρυθμίσεων (factory reset)

Τέλος, ανεξαρτήτως τύπου συναλλαγής (ανέπαφης, μέσω εφαρμογής), όλες οι εντολές πληρωμής συνοδεύονται από το DAN και έναν dynamic κωδικό ασφάλειας που σχετίζεται με την κάθε μία συναλλαγή. Ο κωδικός αυτός είναι μίας χρήσης και κάθε φορά υπολογίζεται από έναν αύξοντα counter ο οποίος αλλάζει σε κάθε συναλλαγή και ένα κλειδί το οποίο παρέχεται στην εφαρμογή πληρωμής (κατά την διάρκεια της εγκατάστασης και ρύθμισης της στην συσκευή μας) και είναι γνωστή στο Payment network και/ή στον πάροχο της κάρτας. Το μοντέλο αυτό tokenization, σταθερό token με dynamic cryptogram, οφείλεται στην συμβατότητα με το μοντέλο της EMVCo.

Για να εισαχθεί ακόμα μεγαλύτερη τυχαιότητα και κατά συνέπεια ασφάλεια στην συναλλαγή, μπορεί να προστεθούν και άλλα δεδομένα στον υπολογισμό αυτών των κωδικών, όπως: ένα τυχαίο νούμερο το οποίο δημιουργείται από την εφαρμογή πληρωμή, ένα τυχαίο νούμερο που δημιουργείται από το τερματικό POS ή ακόμα και ένα νούμερο, δημιουργημένο από τους servers της Apple, κάνοντας ακόμα και το μήκος τους τυχαίο.

Οι κωδικοί αυτοί, αποτελούν ουσιαστικά το πολυσυζητημένο Tokenization που χρησιμοποιεί η Apple για τις αγορές μέσω του Apple Pay. Ο τρόπος δηλαδή με τον οποίο οι συναλλαγές πραγματοποιούνται χωρίς κανένα στοιχείο της κάρτας ή του χρήστη να μην μεταφερθεί σε καμία από τις οντότητες που σχετίζονται με την συναλλαγή όπως ο Merchant, ο Issuer, ο φορέας πληρωμής του εμπόρου κτλ.

5.2.3.2. Ανέπαφη πληρωμή μέσω POS

Οπότε, στην περίπτωση πληρωμής σε POS τερματικό, μόλις η ξεκλείδωτη συσκευή εντοπίσει NFC πεδίο (αν είναι κλειδωμένη, χρειάζεται πίεση δύο φορές του HOME πλήκτρου), εμφανίζει την κάρτα που έχει επιλεχθεί ως default. Εναλλακτικά, μπορεί να γίνει επιλογή άλλης κάρτας από την εφαρμογή Wallet.

Κατόπιν, γίνεται η αυθεντικοποίηση του cardholder μέσω δακτυλικού αποτυπώματος ή του Passcode, όπως αναφέρθηκε παραπάνω. Ακόμα δεν έχει γίνει καμία πληρωμή. Μόλις ολοκληρωθεί η αυθεντικοποίηση, φεύγει το πακέτο πληροφορίας αναφορικά με την κάρτα μας (DAN + dynamic security code) για να προχωρήσει η συναλλαγή. Για ακόμη μία φορά τονίζεται πως, κανείς, ούτε η Apple, ούτε ο Merchant δεν λαμβάνουν πληροφορία για την κάρτα. Η Apple λαμβάνει μια ανώνυμη πληροφορία όπως την ώρα και το μέρος της συναλλαγής, αλλά τίποτα σχετικά με τον χρήστη ή την κάρτα του. Το POS με την σειρά του στέλνει την αίτηση συναλλαγής, μέσω του Acquirer, στον TSP (3), ο οποίος με την σειρά του κάνει την αντιστοίχιση του token με το PAN της κάρτας από το Token Vault του. Μόλις ανασύρει το PAN, μαζί με την αίτηση έγκρισης της συναλλαγής, τα στέλνει στον Issuer. Ο Issuer, αφού εγκρίνει (ή απορρίψει) την συναλλαγή, στέλνει την έγκριση πίσω η οποία φτάνει στο POS μαζί με το token (όπως παρουσιάστηκε η διαδικασία στην περιγραφή του tokenization).

5.2.3.3. Πληρωμή μέσω εφαρμογής

Εν συντομία, όταν ο cardholder επιχειρεί να πληρώσει μέσω εφαρμογών πληρωμής καταστημάτων από το Apple Pay, η Apple λαμβάνει μια κρυπτογραφημένη πληροφορία την

οποία επανακρυπτογραφεί με ένα ειδικό κλειδί συνδεδεμένο με τον Merchant, πριν σταλθεί στον ίδιο τον έμπορο. Πληροφορίες όπως το ποσό της πληρωμής παραμένουν στην Apple, αλλά σε καμία περίπτωση δεν συμπεριλαμβάνονται πληροφορίες σχετικά με την ταυτότητα του cardholder, ούτε καν τι αγόρασε.

Πιο αναλυτικά, όταν μέσα από την εφαρμογή αγοράς γίνει αίτηση για πληρωμή, καλείται ένα API (application programming interface) το οποίο ελέγχει εάν η συσκευή είναι συμβατή με το Apple Pay και εάν ο cardholder έχει κάρτες οι οποίες είναι ικανές να πραγματοποιήσουν πληρωμές στο δίκτυο πληρωμών του εμπόρου. Μόλις γίνει η αυθεντικοποίηση του χρήστη από το Touch ID ή το Passcode, τότε και μόνο τότε η εφαρμογή ζητά πληροφορίες απαραίτητες για την πληρωμή όπως διεύθυνση που θα γίνει η παράδοση και θα φαίνεται στα στοιχεία της χρέωσης.

Η εφαρμογή εν συνεχεία, καλεί μέσω iOS το template sheet όπου συμπληρώνονται στοιχεία όπως χώρα, πόλη και ταχυδρομικός κώδικας ώστε να υπολογιστεί το τελικό ποσό χρέωσης.

Μόλις γίνει η αυθεντικοποίηση από το Touch ID (ή το Passcode) γίνεται ένα session call στους servers της Apple όπου ζητείται και λαμβάνεται ένα nonce. Το nonce μαζί με τα δεδομένα της συναλλαγής πηγαίνουν στο Secure Element όπου εκεί, όπως αναφέρθηκε και παραπάνω, κρυπτογραφούνται από το DAN και ένα counter για την αποφυγή replay επίθεσης. Δημιουργείται το λεγόμενο Payment Credential και στέλνετε στους Servers της Apple όπου αποκρυπτογραφείται και ελέγχεται η γνησιότητα του κρυπτογραφικού Nonce. Εδώ πρέπει να γίνει μία παρατήρηση, η συναλλαγή μέσω App θεωρείται card-not-present συναλλαγή. Οπότε, η συναλλαγή για να ολοκληρωθεί ζητάει μια έξτρα πληροφορία την οποία λαμβάνει από την πλατφόρμα του 3DS(Three Domain Secure), (VBV, Mastercard Secure-Code, Amex Safekey) η οποία στέλνεται μαζί με το υπόλοιπο payment token (3).

Εάν πιστοποιηθεί η γνησιότητα του, τα credential κρυπτογραφούνται εκ νέου, με ένα κλειδί που σχετίζεται αποκλειστικά με τον Merchant. Ο Merchant με την σειρά του τα αποκρυπτογραφεί με το ιδιωτικό του κλειδί και προχωρά στην επιβεβαίωση/επεξεργασία της παραγγελίας. Όπως και πριν, ο Merchant δεν έχει κανένα στοιχείο της φυσικής κάρτας του χρήστη όπως αριθμός ή όνομα κατόχου παρά μόνο στοιχεία αποστολής και τιμολόγησης. Εάν η εφαρμογή είναι προγραμματισμένη έτσι ώστε να ζητά επιπλέον στοιχεία προς αποστολή στον

έμπορο, με σκοπό την περαιτέρω ταυτοποίηση της συναλλαγής, τότε τα στοιχεία αυτά στέλνονται μαζί με τα υπόλοιπα που αναφέρθηκαν παραπάνω στο Secure Element προς κρυπτογράφηση. Στο τελικό πακέτο πληροφορίας που λαμβάνει ο Merchant, θα υπάρχει και ένα hash αυτής της έξτρα ενημέρωσης το οποίο και θα συγκρίνει με το Hash από έλαβε από την εφαρμογή.

5.2.3.4. Λειτουργία Reward καρτών

Τέλος για να καλυφθεί και μία ανάγκη που υπάρχει στο καταναλωτικό κοινό ήδη, από την έκδοση iOS 9 και μετά, το Apple Pay υιοθέτησε το πρωτόκολλο VAS (valued added service) για την μετάδοση πληροφοριών σε reward κάρτες εμπόρων από NFC POS τερματικά. Το VAS (ή Mobile VAS όπως μπορεί να το βρει κάποιος) χρησιμοποιείτε στις τηλεπικοινωνίες για μη βασικές λειτουργίες (πχ δεν χρησιμοποιείτε για πληρωμές)

Λειτουργεί σε μικρές αποστάσεις λόγω NFC. Για την περίπτωση που εξετάζεται, δηλαδή για την μεταφορά πχ πόντων στην κάρτα ενός καταστήματος, το τερματικό του καταστήματος στέλνει ένα request για τέτοια κάρτα και ο cardholder καλείται να απαντήσει θετικά. Εάν από την μεριά του Merchant υποστηρίζεται κρυπτογράφηση, τα δεδομένα της κάρτας κρυπτογραφούνται με ένα timestamp, ένα τυχαίο κλειδί ECDH P-256 (Elliptic Curve Diffie-Hellman, μία παραλλαγή του κλασσικού Diffie -Hellman πρωτοκόλλου το οποίο χρησιμοποιεί κρυπτογραφία ελλειπτικής καμπύλης) μίας χρήσης και το public κλειδί του Merchant και στέλνονται στο τερματικό.

5.3. Προβληματισμοί σχετικά με το Apple Pay

Αν και η αρχιτεκτονική ασφάλειας το Apple Pay φαίνεται εντυπωσιακή, διάφορα θέματα έχουν προκύψει τους πρώτους μήνες της χρήσης του. Το σημαντικότερο ίσως από όλα όμως, φαίνεται να μην έχει να κάνει με το σύστημα ασφάλειας του Apple Pay όπως είναι στημένο στην συσκευή, ούτε καν στις ίδιες τις συναλλαγές. Το κενό που έχει παρατηρηθεί και έχει επιφέρει προβληματισμό αλλά και τα πρώτα φαινόμενα fraud, βρίσκεται στον μηχανισμό ταυτοποίησης του χρήστη από τις τράπεζες, όταν δηλώνεται μία καινούργιάς κάρτας προς χρήση μέσω Apple Pay.

Υπάρχουν τρείς τρόποι για να προχωρήσει η ταυτοποίηση ενός χρήστη κατά την διαδικασία δήλωσης μια κάρτας στο Apple Pay,

- Το Green Path, στο οποίο ο Issuer δεν ζητάει επιπλέον διαπιστευτήρια από τον αιτών για την κάρτα, μετά το πέρας των τριών session calls που αναφέρθηκαν παραπάνω.
- Το Red Path, στο οποίο ο Issuer κρίνει ότι υπάρχει πρόβλημα με την ταυτοποίηση των δεδομένων και απορρίπτει την κάρτα για χρήση στο Apple Pay
- Το Yellow Path, στο οποίο Ο Issuer κρίνει ότι είναι απαραίτητο να γίνει περαιτέρω ταυτοποίηση από τον αιτών, για να προχωρήσει στην έγκριση.

Εδώ ακριβώς είναι που δημιουργείται και το θέμα, στον τρόπο και συχνότητα χρήσης του Yellow Path. Πρώτα όμως, κρίνεται σκόπιμο να γίνει μια σύντομη ανασκόπηση στο πως γίνεται η απάτη στις κάρτες γενικά. Όταν γίνεται υποκλοπή στοιχείων καρτών, συνήθως μέσω malware στα POS ή με breach των Servers που κρατούνται δεδομένα καρτών, προκύπτουν "dumps" αρχείων που μπορούν εύκολα να αγοραστούν σε sites. Αντίστοιχα, γίνεται υποκλοπή CVV κωδικών καρτών από online sites καταστημάτων. οπότε, αν θεωρηθεί ότι κάποιος είναι απατεώνας και θέλει να κάνει αγορές σε φυσικό κατάστημα, αγοράζει κλεμμένα "dumps" και δημιουργεί δική του κάρτα αφού έχει όλα τα στοιχεία, ενώ αντίστοιχα για online αγορές, αγοράζει ένα CVV μαζί με το οποίο του παρέχουν το PAN της κάρτας, ημερομηνία λήξης και όνομα κατόχου. Όλα αυτά με κόστος που δεν ξεπερνά τα 5 ευρώ.

Αυτά τα περιστατικά δεν είναι καινούργια καθώς τέτοιες υποκλοπές έχουν γίνει σε μεγάλη κλίμακα στο παρελθόν. Αυτό που αλλάζει τώρα είναι ότι πλέον, με το Apple Pay, δεν χρειάζεται καν η δημιουργία φυσικής κάρτας για να προβεί κάποιος σε συναλλαγές. Απλά δηλώνεται στο Apple Pay και απαιτείται μόνο να έχει κάποιος στην κατοχή του τα στοιχεία της που μπορούν να προκύψουν και από έναν χακαρισμένο λογαριασμό iTunes.

Το πρόβλημα του Yellow Path, είναι ότι πρώτον δεν είναι αναγκαστικό αλλά είναι στην διακριτική ευχέρεια της κάθε τράπεζας εάν θα το χρησιμοποιήσει και δεύτερον ότι ο τρόπος που γίνεται είναι ελλιπής.

Η πλειοψηφία των τραπεζών, χρησιμοποίησαν τα Call Center τους ως μέσο ταυτοποίησης του χρήστη, συνήθως ρωτώντας τον για τα τελευταία 4 ψηφία του SSN (social security number, για την Αμερική), του οποίου η υποκλοπή είναι ένα από τα πιο γρήγορα ανερχόμενα εγκλήματα στην Αμερική (43). Επιπλέον, η ίδια η φύση των call centers μπορεί να δημιουργήσει πρόβλημα λόγω του ανθρώπινου παράγοντα (βλέπε social engineering). Σε

αρκετές περιπτώσεις οι ίδιοι οι απατεώνες έχουν επικοινωνήσει με τα call centers για να “ενημερώσουν” ‘ότι θα λείψουν σε ταξίδι ώστε να μην προκαλέσει υποψία η αίτηση για δήλωση μια κάρτας στο Apple Pay από χώρα διαφορετική από την χώρα έκδοσης.

Πάνω στο στάδιο της ταυτοποίησης του cardholder, ενδιαφέρον παρουσιάζει ένα περιστατικό που παρατηρήθηκε στην Βρετανία, όπου στην προσπάθεια να προσθέσουν κάρτα η οποία εκδόθηκε από την HSBC Βρετανίας σε λογαριασμό Apple Pay ενώ ο cardholder ήταν εκτός Βρετανίας, υπήρξε απόρριψη της κάρτας. Αυτό φυσικά και δεν θα ήταν πρόβλημα με το σκεπτικό ότι η απόρριψη έγινε ύστερα από έλεγχο της περιοχής που βρίσκεται ο cardholder μέσω των “Location Services” και ακυρώθηκε για λόγους ασφάλειας. Όμως, όταν ο cardholder απενεργοποιείσαι τα “Location Services” και επέλεξε ένα “UK VPN” μέσα από τα “Settings” και επανέλαβε την διαδικασία, η κάρτα έγινε δεκτή (44). Οπότε, μπορεί ουσιαστικά από τον ίδιο τον χρήστη να προσπεραστεί μία διαδικασία δυναμικής ταυτοποίησης των PII δεδομένων του χρήστη μέσω της περιοχής που γίνεται διαδικασία αίτησης.

Σε τεχνικό επίπεδο, πάντα υπάρχει ο κίνδυνος μέσω ενός malware να υποκλαπούν δεδομένα όχι αποθηκευμένα, αλλά την ώρα που περνάνε στη συσκευή, όπως η φωτογραφία της κάρτας την ώρα που γίνεται η εισαγωγή της φωτογραφίας ή την ώρα που πληκτρολογούμε τα στοιχεία. Σε περίπτωση επιστροφής χρημάτων (refund) θα χρειαστεί μπορεί να απαιτηθεί να δώσω στον ταμία τα τελευταία 4 ψηφία του DAN της κάρτας μου. Και πάλι, δεν προσφέρονται στοιχεία από την πραγματική κάρτα, αλλά τα 4 ψηφία δεν παύουν να είναι δεδομένο που προσφέρει πληροφορία για την κάρτα.

Επιπλέον, η Apple ζητάει για την υπηρεσία της αμοιβή 0.15% από τις τράπεζες (τις card issuer τράπεζες) για κάθε συναλλαγή που γίνεται μέσω Apple Pay. οι τράπεζες όμως έχουν ήδη πολύ μικρό περιθώριο κέρδους από το ποσό που εισπράττουν από τις Acquirer τράπεζες που συνεργάζεται ο Merchant (περίπου 0.20% για debit cards και 0.30 για credit cards), οπότε με αυτό το fee μειώνεται ακόμα περισσότερο.

6. SAMSUNG PAY

6.1. Εισαγωγή

Στις αρχές του 2015, η Samsung ανακοίνωσε την νέα της εφαρμογή για mobile πληρωμές, την Samsung Pay. Η εφαρμογή έκανε το ντεμπούτο της στην Ν. Κορέα τον Αύγουστο και στην Αμερική τέλη Σεπτέμβρη.

Ταχύτητα στη συναλλαγή, ευελιξία ως προς τον πάροχο της κάρτας και ο ισχυρισμός ότι δουλεύει σχεδόν στο 90% των εμπόρων είναι τα όπλα με τα οποία η Samsung προωθεί τα προϊόν της. Κλειδί στην προώθηση της παίζει το γεγονός ότι ως μέθοδος πληρωμής είναι συμβατή τόσο σε τερματικά POS με NFC τεχνολογία αλλά και στα συμβατικά με mag-stripe/EMV τεχνολογία. Το Samsung Pay είναι εφαρμογή, η οποία πολύ εύκολα κατεβαίνει μέσα από το Google Pay. Οι συσκευές με τις οποίες για την ώρα είναι συμβατή είναι οι ναυαρχίδες της εταιρίας (Samsung Galaxy S6 και νεότερα μοντέλα και Samsung Galaxy Note 5), αν και η εταιρία υποσχέθηκε ότι θα υποστηρίξει στο μέλλον και τα πιο low-end μοντέλα που θα κυκλοφορήσουν. Η εφαρμογή είναι αποκλειστική για χρήστες κινητών συσκευών Samsung και δεν υπάρχει κάποιο άμεσο πλάνο για άλλες εταιρίες. Εξαίρεση αποτελεί η αποστολή gift cards από Samsung Pay σε χρήστες άλλων συσκευών.

Αναφέρθηκε παραπάνω ότι το Samsung Pay, θα επιτρέπει συναλλαγές τόσο σε συμβατικά POS τερματικά όσο και σε NFC enabled. Είναι μάλιστα, προς το παρών, η μοναδική εταιρία που το καταφέρνει. Το μοναδικό της αυτό χαρακτηριστικό έγινε εφικτό μετά την εξαγορά της εταιρίας LoopPay, η οποία λίγα μόλις χρόνια πριν είχε αναπτύξει την, πατενταρισμένη πλέον, τεχνολογία MST (magnetic secure transmission), μία μέθοδο με την οποία το κινητό μέσω μιας έξτρα θήκης, μπορούσε να μιμηθεί την λειτουργία μιας τυπικής mag-stripe/EMV κάρτας. Τώρα πλέον, η Samsung έχει ενσωματώσει την τεχνολογία αυτή στα τελευταία high-end κινητά της(Samsung Galaxy S6 και πάνω), χωρίς την ανάγκη χρήσης κάποιας έξτρα θήκης ή gadget δίνοντας στις συσκευές αυτές την ελευθερία μέσω του Samsung Pay να εκτελούν συναλλαγές σε όσα καταστήματα έχουν POS τερματικά NFC ή συμβατικά.

Πριν ξεκινήσει η παραμετροποίηση της εφαρμογής, θα πρέπει να διευκρινιστεί πως το κινητό τηλέφωνο, ο πάροχος κινητής τηλεφωνίας που θα χρησιμοποιηθεί και το Payment Network στο οποίο ανήκει η κάρτα, είναι συμβατά με το Samsung Pay. Η εταιρία έχει

εξασφαλίσει συνεργασία με την Visa, Mastercard και American Express στην Αμερική, με ένα μεγάλο αριθμό τραπεζών και τα (προϊόντα κάρτες τους) συνεχώς αυξανόμενο, αλλά ακόμα περιορίζεται στην Αμερική, αν και υπάρχουν πλάνα επέκτασης στην Κίνα στις αρχές του 2016 και υπάρχει κινητικότητα και με την Visa Ευρώπης.

6.2. Συνοπτική παρουσίαση του MST

Ως MST (magnetic secure transmission) ορίζεται η τεχνολογία που ανέπτυξε η LoopPay, για την οποία έχει κατοχυρώσει πατέντα (45), με την οποία καταφέρνει να προσομοιώσει την συμπεριφορά μια μαγνητικής κάρτας. Τα τεχνικά στοιχεία που κυκλοφορούν αφορούν ξεχωριστές (add-on) συσκευές της LoopPay και αυτές λειτουργούν σε συνδυασμό με ένα κινητό αλλά δεν βρέθηκαν αρκετά στοιχεία αναφορικά με την υλοποίηση της στα κινητά και tablets της Samsung.

Η ιδέα περιλαμβάνει την κινητή συσκευή με την εφαρμογή wallet και μια συσκευή για την συλλογή, αποθήκευση και μετάδωσε των δεδομένων της μαγνητικής ταινίας. Η συσκευή αυτή (MST) στη παρούσα φάση είναι σε εξωτερική μορφή και όχι embedded στο τηλέφωνο. Το MST μπορεί να επικοινωνήσει με την συσκευή σε διάφορα modes.

- Initialize & Reset mode, όπου εδώ γίνεται η σύζευξη ή διαχωρισμός μιας συσκευής MST με ένα συγκεκριμένο mobile wallet λογαριασμό και θα επιτρέπεται ένα MST ανά λογαριασμό.
- Load-Delete Card mode, όπου εδώ φορτώνει τα στοιχεία της κάρτας περνώντας από ένα εξωτερικό Module μαγνητικού αναγνώστη και αποθηκεύει τα στοιχεία είτε στη μνήμη είτε στο secure element.
- Transmit & Use mode, επιτρέπει να επιλεχθεί ποια κάρτα θα χρησιμοποιηθεί για πληρωμή ή ποια θα είναι η default για μελλοντικές πληρωμές.
- POS Card Read mode, επιτρέπει να διαβαστεί μια κάρτα από τον μαγνητικό αναγνώστη του MST, και να μεταδώσει τα δεδομένα αυτά σε μια POS-like, check-out εφαρμογή του εμπόρου από την τηλεφωνική συσκευή που είναι

συνδεμένο και μετά στον Acquirer (τραπεζικό συνεργάτη) του εμπόρου. Έτσι, προσομοιώνει ένα card-present περιβάλλον.

Η μοναδική παραφωνία που παρουσίαζε το LoopPay MST, ήταν η συμπεριφορά του σε EMV κάρτες. Όταν παρουσιαζόταν με αποθηκευμένη προς χρήση μια EMV κάρτα, σε POS τερματικό όπου είναι μεν MSR αλλά το EMV ήταν ενεργό, εμφανιζόταν μήνυμα ότι η συναλλαγή πρέπει να γίνει με την φυσική κάρτα. Αυτό συνέβαινε διότι στα track data των EMV καρτών υπάρχει ένας κωδικός υπηρεσίας 201 ο οποίος αποτρέπει στις EMV κάρτες να διαβαστούν από έναν MSR αναγνώστη σε ένα EMV enabled POS. Αυτό δεν έχει παρουσιαστεί σαν πρόβλημα στην υλοποίηση της Samsung.

6.3. Δήλωση κάρτας με το Samsung Pay

Επόμενο βήμα, αφού κατέβει και εγκατασταθεί η εφαρμογή στην συσκευή, είναι να κάνει log in ο cardholder στην εφαρμογή (χρειάζομαι Samsung Account). Ως μέθοδος ασφάλειας προτείνεται το δακτυλικό αποτύπωμα. Εάν δεν έχει αποθηκευτεί, η εφαρμογή ζητάει να οριστεί εκείνη τη στιγμή. Θα χρειαστεί να γίνει επαφή του δάκτυλου λίγες φορές επάνω στο “Home Key” κουμπί μέχρι να φτάσει η ένδειξη της καταχώρησης του αποτυπώματος στο 100%. Στην συνέχεια ζητάει να οριστεί και ένα back-up password και τέλος δηλώνεται ένα 4ψήφιο **Samsung Pay pin**, για την περίπτωση που δεν θέλει ο cardholder ή δεν μπορεί να χρησιμοποιήσει δακτυλικό αποτύπωμα. Για να γίνει προσθήκη μίας κάρτας στον λογαριασμό του cardholder, μέσα από την εφαρμογή, επιλέγει ADD ή Add a credit or debit card (εάν είναι η πρώτη κάρτα που περνάει). Αμέσως, εμφανίζει ένα πλαίσιο στην οθόνη στο οποίο θα πρέπει να ευθυγραμμιστεί η κάρτα που θέλουμε να προσθέσουμε μπροστά από την κάμερα του κινητού. Αυτόματα, θα εισαχθούν το νούμερο της κάρτας και η ημερομηνία λήξης. Συμπληρώνει τα υπόλοιπα στοιχεία και πατάει next (σε αυτό το βήμα, δηλώνεται και το CVV νούμερο) και πατάει next. Αν ζητηθεί, δηλώνει και την διεύθυνση χρέωσης. Ο αριθμός της κάρτας στέλνεται κρυπτογραφημένος προς τους tokenization servers του δικτύου πληρωμής που ανήκει η κάρτα. Ελέγχεται το 1^{ο} πρώτο βήμα από τον Issuer και φέρνει μπροστά στην οθόνη τους όρους χρήσης της κάρτας από τον Issuer. Εάν γίνουν δεκτοί, το επόμενο βήμα είναι να γίνει επιλογή κάποιας μεθόδου πιστοποίησης (sms, email ή τηλέφωνο στο call center του Issuer). Ανάλογα με την μέθοδο, ο cardholder παραλαμβάνει ένα OTP το οποίο το στο τελευταίο βήμα για να ολοκληρώσει την διαδικασία. Ο Issuer και το Payment Network (Visa, Mastercard κτλ.) ελέγχει

όλα τα στοιχεία και εγκρίνει (ή όχι) την κάρτα για χρήση στο Samsung Pay. Αν όλα κυλήσουν ομαλά, το δίκτυο της κάρτας αναθέτει στην συσκευή ένα token το οποίο θα έχει τον ρόλο του αριθμού της κάρτας για τις συναλλαγές μέσω Samsung Pay. Ο πραγματικός αριθμός της κάρτας δεν δηλώνεται στους servers της Samsung, μόνο ένα αντίγραφο του token. Σε αυτό το σημείο να αναφέρουμε ότι στην διαδικασία δήλωσης καρτών της Samsung Pay, βρίσκουμε πάλι τα τρία μονοπάτια-σενάρια που αναφέρθηκαν και στην περίπτωση της Apple,δηλαδή το Green Path, Yellow Path και Red Path, όπου στο 1ο υπάρχει επικύρωση από την τράπεζα χωρίς επιπλέον credential, στο 2ο ζητάει επιπλέον αυθεντικοποίηση με τις μεθόδους που αναφέραμε πριν, ενώ στο Red Path δεν επιτρέπει την προσθήκη της συγκεκριμένης κάρτας στο Samsung Pay.

Αντίστοιχα, για να αφαιρεθεί μια κάρτα, μέσα από την εφαρμογή γίνεται επιλογή της κάρτας προς διαγραφή, ο cardholder επιλέγει “More” → “Delete Card” → “Delete”. Θα ζητηθεί Pin ή δακτυλικό αποτύπωμα για επιβεβαίωση. Μόλις γίνει η διαγραφή θα αφαιρεθεί και το token που αντιπροσώπευε την κάρτα μας από την συσκευή.

Για να δηλωθεί μια κάρτα, θα πρέπει να υπάρχει πρόσβαση σε Internet, για να γίνουν οι απαραίτητες πιστοποιήσεις. Η ίδια κάρτα, γίνεται να είναι δηλωμένη σε παραπάνω από μία συσκευή, το όριο το ορίζει (εάν υπάρχει) ο Issuer. Μπορούν να υπάρξουν μέχρι και 10 κάρτες debit ή credit δηλωμένες στη συσκευή, αλλά δεν έχει όριο για gift cards, ενώ η δήλωση credit καρτών που εκδίδονται από Merchants(store credit cards), γίνονται δεκτές περιορισμένα

6.4. Διαδικασία Πληρωμής με το Samsung Pay

Για να γίνει μία πληρωμή, «σαρώνεται» η οθόνη της συσκευής από κάτω προς τα πάνω για να εμφανίσει τις κάρτες στην οθόνη. Αυτό μπορεί να γίνει ακόμα και όταν η συσκευή είναι κλειδωμένη. Δεν υπάρχει η δυνατότητα να δηλωθεί default κάρτα στην εφαρμογή, θα εμφανίζεται πρώτη αυτή που είχε χρησιμοποιηθεί τελευταία φορά. Μετακινώντας το δάκτυλο πάνω στη οθόνη αριστερά ή δεξιά εμφανίζονται και όποιες άλλες κάρτες έχουν δηλωθεί στην συσκευή και επιλέγεται ποια θα χρησιμοποιήσει ο cardholder για την συναλλαγή. Όταν ο ταμίας είναι έτοιμος, πιέζει το “Home Key” για να προχωρήσει στην πληρωμή (ή εισάγει το 4ψήφιο Pin). Ανάλογα με το τερματικό POS (εάν είναι NFC enabled ή κλασσικό card reader χάρη στης τεχνολογία MST), θα πλησιάσει το τηλέφωνο είτε κοντά στον δέκτη NFC ή στην είσοδο της κάρτας. Απαιτείται να υπάρχει σύνδεση στο internet για να πραγματοποιηθούν συναλλαγές με το Samsung Pay, αν και δίνεται η δυνατότητα για μέχρι και 10 συναλλαγές σε off-line περιβάλλον.

Πληρωμές με Samsung Pay δεν μπορούν γίνουν σε σημεία όπου εάν είχα κάρτα, θα έπρεπε να μπει αναγκαστικά μέσα σε αναγνώστη (πχ σε ATM). Πληρωμές δεν μπορούν να γίνουν επίσης, προς το παρών, online μέσα από apps των εμπόρων. Δίνεται η δυνατότητα ελέγχου του πρόσφατου ιστορικού των αγορών μέχρι και ένα μήνα πίσω, από την ημερομηνία της συναλλαγής.

Στην περίπτωση που χρειαστεί να γίνει επιστροφή του προϊόντος της συναλλαγής και να γίνει κάποιο refund, είναι πιθανό να ζητηθεί να γίνει παρουσίαση των τελευταίων τεσσάρων ψηφίων από τον dummy αριθμό της κάρτας. Για να εντοπιστεί ο αριθμός αυτός, ο cardholder επιλέγει την κάρτα μέσα από την εφαρμογή και εκεί διαβάζει το πεδίο που λέει Digital card Number.

Αν υπάρξει απώλεια ή κλοπή της συσκευής, μέσω της πλατφόρμας “Find my Device” υπάρχει η δυνατότητα remotely να κλειδώσει η συσκευή, να γίνει διαγραφή των καρτών που έχουν περάσει στο Samsung Pay στην συσκευή, ή αν θεωρηθεί απαραίτητο να πραγματοποιηθεί factory reset σε όλη τη συσκευή. Για επιπλέον ασφάλεια, αν δηλωθεί διαγραφή των καρτών, η Samsung Pay επικοινωνεί με τον Issuer ώστε να μην κάνει δεκτές συναλλαγές από την συγκεκριμένη συσκευή.

6.5. Μοντέλο Ασφάλειας του Samsung Pay

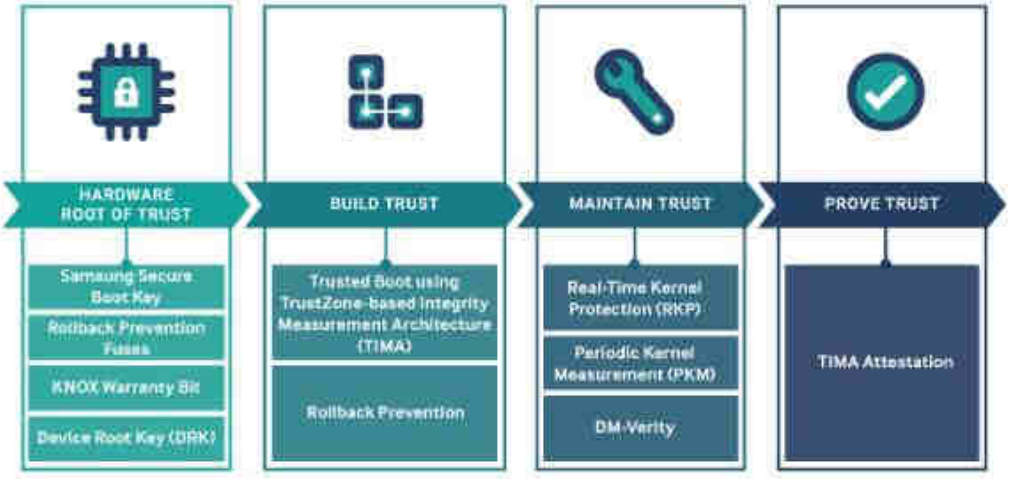
Στο κομμάτι της ασφάλειας, η Samsung φαίνεται να αφήνει ανοιχτό το δίλλημα Secure Element ή HCE καθώς ενσωματώνει και τις δύο τεχνολογίες αφήνοντας τις τράπεζες να επιλέξουν πως και που θα αποθηκεύουν τα tokens των καρτών. Το secure element για τις συσκευές της σειράς Galaxy S6 τις προμηθεύτηκε από την Oberthur (46) (σε συνεργασία με την Infineon) το οποίο έχει την κωδική ονομασία **Pearl** (ή SLE 97). Ένα από τα σημαντικότερα χαρακτηριστικά του είναι το DCLB (digital contactless bridge) interface, το οποίο είναι ρυθμισμένο ώστε να συνεργάζεται ιδανικά με NFC enabled POS.

6.5.1. Εισαγωγή στο Samsung Knox

Η στρατηγική της επιλογή ωστόσο, ήταν η ενσωμάτωση της πλατφόρμας **Samsung Knox,** σε όλες τις συσκευές που υποστηρίζουν το Samsung Pay. Το Samsung Knox είναι μία πλατφόρμα ασφάλειας σε Hardware και Software επίπεδο και αρχικά είχε προωθηθεί για εταιρική χρήση, λαμβάνοντας υπόψη το όλο και αυξανόμενο μοτίβο του BYOD(bring your own

device) στις εταιρίες παρέχοντας υπηρεσίες mobile security, ως αντίπαλο δέος στο BlackBerry Balance, μια υπηρεσία που ξεχωρίζει στην συσκευή δεδομένα και εφαρμογές σε 1.προσωπικές και 2.εργασίας. Η αποδοχή που είχε ήταν τέτοια, σε σημείο που η NSA(US National Security Agency) το 2014 ενέκρινε (47)την χρήση συσκευών Samsung οι οποίες υποστηρίζονται από την πλατφόρμα Knox.

Η Εφαρμογή Samsung Pay και κατά επέκταση τα δεδομένα των πληρωμών ενός χρήστη, αλλά και η διαχείριση του δακτυλικού αποτυπώματος και η διαδικασία επικύρωσης με την χρήση του, είναι πλέον κάτω από την "ομπρέλα" του Knox. Το κυρίως πρόβλημα που καλείται να λύσει το Knox (48) σε επίπεδο ενός απλού χρήστη είναι η έλλειψη εμπιστοσύνης (**Trust**) στο Android περιβάλλον, η επιβεβαίωση δηλαδή ότι η συσκευή λειτουργεί βάση ελεγμένων και πιστοποιημένων συνθηκών. Για το πλειονότητα των εφαρμογών και λειτουργιών της συσκευής, η ορθή λειτουργία πιστοποιόταν από την κρυπτογραφική υπογραφή του κάθε τμήματος των εφαρμογών. Οι Android συσκευές ως open source λειτουργικό ήταν πάντα ανοιχτές σε exploitation και μεγάλο ποσοστό των χρηστών είχαν προβεί σε rooting της συσκευής επηρεάζοντας πολλές παραμέτρους της λειτουργίας της. Τα βήματα που ακολουθεί το Knox για την διαχείριση της είναι, όπως φαίνεται και στο σχήμα **(εικόνα_19)**



Εικόνα 19 Τρόπος Λειτουργίας του Knox, by Samsung Knox-Security Solution whitepaper

- Hardware Root of Trust, πιστοποιώντας ότι τα κρυπτογραφικά κλειδιά και οι συναρτήσεις από τις οποίες προέκυψαν, μπορούν να επιβεβαιωθούν από κάποιες σταθερές, αμετάβλητες τιμές οι οποίες είναι αποθηκεμένες στο hardware.

- Build Trust, επιτρέποντας την φόρτωση μόνο επιβεβαιωμένων system-critical εφαρμογών
- Maintain Trust, παρακολουθώντας και επιβεβαιώνοντας ότι οι system-critical εφαρμογές δεν αλλάζουν από την στιγμή που θα φορτωθούν
- Prove Trust, όταν και όποτε ζητηθεί, θα πρέπει το σύστημα να μπορεί να αποδείξει πως ότι είναι φορτωμένο και τρέχει πάνω στο σύστημα, είναι επικυρωμένο.

6.5.2. Ανάλυση του Samsung Knox

Θα παρουσιαστεί πως το Knox υλοποιεί βήμα προς βήμα την αρχιτεκτονική του Trust, ξεκινώντας από το επίπεδο του Hardware, προχωρώντας στην διαδικασία του Boot, συνεχίζοντας στην διατήρηση του Trust όσο η συσκευή λειτουργεί και τέλος πως πιστοποιεί την ορθή λειτουργία του σε τρίτους (για παράδειγμα, κατά την συναλλαγή μέσω Samsung Pay).

Σε μία κλασσική συσκευή Android, ο bootloader δεν πιστοποιεί την ταυτότητα του kernel στην συσκευή. Αυτό δίνει την ευχέρεια σε έναν απλό χρήστη να παρέμβει στον kernel(rooting), βάζοντας μια άλλη έκδοση, κάτι που του δίνει δικαιώματα superuser σε όλη τη συσκευή. Αυτό σημαίνει ότι αν στη συσκευή μπει κάποιο malware, αυτόματα είναι εκτεθειμένα όλα τα τμήματα του λόγω των elevated δικαιωμάτων που έχει πλέον ο cardholder. Επιπλέον, μετά το system boot, το λειτουργικό δεν ελέγχει σε όλη την διάρκεια της λειτουργίας της συσκευής αν έχουν γίνει παρεμβολές στον kernel ή και στο ίδιο το λειτουργικό. Γι’ αυτό ακολουθεί πλέον με το Knox τα παρακάτω βήματα ώστε να εξασφαλίσει όχι μόνο ασφαλή εκκίνηση αλλά και συνεχή παρακολούθηση και έλεγχο.

- Hardware Root Of Trust

Τα τμήματα που εμπλέκονται είναι τα παρακάτω,

Device-Unique Hardware Key (DUHK), ένα μοναδικό, συμμετρικό κλειδί το οποίο ενσωματώνεται στη συσκευή από κατασκευής της. Είναι προσβάσιμο μόνο από ένα hardware κρυπτογραφικό στοιχείο και δεν επικοινωνεί με καμία εφαρμογή. Μπορεί μόνο να ζητηθεί από το DUHK κρυπτογραφήσει/αποκρυπτογραφήσει δεδομένα. Τα δεδομένα αυτά, γίνονται bound

πλέον στην συσκευή καθώς δεν μπορούν να αποκρυπτογραφηθούν αλλού. Συνήθως χρησιμοποιήται για την κρυπτογράφηση άλλων κλειδιών.

Samsung Secure Boot Key (SSBK), είναι ένα ασύμμετρο ζεύγος κλειδιών. Το ιδιωτικό κλειδί χρησιμοποιήται για να κάνει sign τους δευτερεύον και application bootloaders. Το δημόσιο κλειδί αποθηκεύεται σε μια One-time προγραμματισμένη ασφάλεια, την ώρα της κατασκευής και χρησιμοποιήται από τη Secure Boot διαδικασία, ώστε να επιβεβαιώσει ότι κάθε τμήμα που φορτώνεται είναι πιστοποιημένο.

RP Fuses (Roll Back Prevention Fuses), είναι hardware ασφάλειες στις οποίες είναι αποτυπωμένο οι ελάχιστα αποδεκτές εκδόσεις των bootloaders. Η version αποτυπώνεται από κατασκευής και ανανεώνεται με τα software updates οπότε εκδόσεις που μέχρι πρότινος ήταν αποδεκτές, είναι πιθανό ύστερα από κάποιο update να πάψουν να γίνονται δεκτές.

Knox Warranty Fuse, άλλη μία one-time programmable ασφάλεια, η οποία ελέγχει εάν κατά την έναρξη τρέχουν πράγματα που δεν θα έπρεπε, ή αντίθετα εάν έχουν απενεργοποιηθεί security features που δεν θα έπρεπε πχ SELinux. Αν συμβεί κάτι τέτοιο, η ασφάλεια ενεργοποιείται και η συσκευή δεν μπορεί να τρέξει στο Secure περιβάλλον της και ο cardholder δεν έχει πρόσβαση σε ότι δεδομένα και εφαρμογές υπάρχουν εκεί.

ARM Trust-Zone Secure World, χάρη στη αρχιτεκτονική Trust-Zone των καινούργιων ARM επεξεργαστών (49), υπήρχε η δυνατότητα συνύπαρξης δύο διαφορετικών κόσμων σε μια πλατφόρμα, του Normal World και του Secure World. Στο secure world, έχουμε πρόσβαση μόνο στο κομμάτι της μνήμης, επεξεργαστικών πόρων και εφαρμογών που έχουν χαρακτηριστεί ως Secure. Το Secure World τμήμα έχει πιο privileged δικαιώματα από το Normal world και μπορεί να έχει πρόσβαση στις εφαρμογές και τα αρχεία του αλλά όχι το ανάποδο.

Bootloader ROM, είναι το τμήμα της ROM μνήμης στο οποίο είναι αποθηκεμένος ο primary Bootloader (PBL) ο οποίος αποτελεί τον πρώτο κωδικό που τρέχει κατά την διαδικασία έναρξης.

Device Root Key (DRK), είναι ένα μοναδικό, ασύμμετρο ζεύγος κλειδιών, υπογεγραμμένο από το root κλειδί της Samsung, βασισμένο πάνω σε x.509 πιστοποιητικά (έχουν να κάνουν με PKI-public key infrastructure και PMI-privilege management infrastructure, με σκοπό να αποδειχθεί ότι το ζεύγος DRK είναι όντως της Samsung). Το DRK χρησιμοποιείται για να υπογράφει

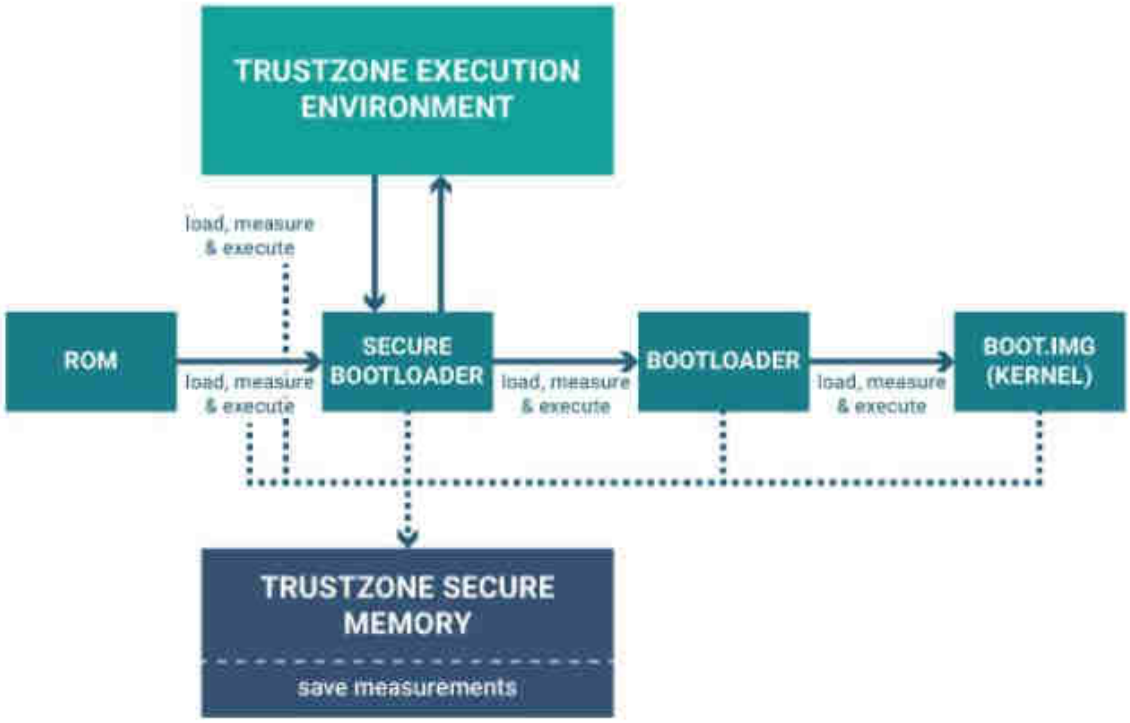
κλειδιά για άλλες διαδικασίες που μπλέκονται στο Knox και πιστοποιεί την αλυσίδα Trust σε όλη την διαδικασία.

- Build-Establishing Trust

Στο λειτουργικό Android, η διαδικασία εκκίνησης ξεκινά με την φόρτωση του PBL από την Bootloader ROM. Μετά το πρώτο βήμα της εκκίνησης, καλείται ο secondary bootloader στην RAM από το File System και εκτελείται. Επειδή είναι πολύ πιθανό να υπάρχουν πολλοί secondary bootloaders, ο επόμενος μπαίνει σε λειτουργία αφού πρώτα τελειώσει ο προηγούμενος. Τελευταίος είναι ο application bootloader, ο οποίος φορτώνει και το λειτουργικό σύστημα. Η διαδικασία αυτή της εκκίνησης ονομάζεται boot chain (αλληλουχία εκκίνησης). Ας δούμε πάνω εδώ πως καταφέρνει το Knox να χτίσει και να εδραιώσει Trust.

Secure Boot, πάνω στην διαδικασία φόρτωσης, το κάθε κομμάτι που φορτώνεται είναι υπεύθυνο για την πιστοποίηση του επόμενου. Το κάθε κομμάτι της διαδικασίας είναι signed από την αρχή χρησιμοποιώντας το κλειδί SSBK που αναφέραμε παραπάνω. Εάν ένα βήμα της εκκίνησης δεν πιστοποιηθεί, η διαδικασία φόρτωσης σταματά. Ας λάβουμε υπόψη μας, ότι το πρώτο βήμα στην εκκίνηση γίνεται από τον PBL μέσα στην ROM, οπότε το chain of trust χτίζεται από κάτι αμετάβλητο. Ο μόνος τρόπος για να παραποιηθεί είναι να υπάρξει παρέμβαση στο hardware.

TIMA (TrustZone-Based Integrity Measurement Architecture) Boot, στο Trusted Boot, κάθε κομμάτι εκκίνησης χρησιμοποιώντας ένα αλγόριθμο SHA 256, υπολογίζει για το επόμενο κομμάτι που θα φορτωθεί το HASH του και το αποθηκεύει σε ένα τμήμα της μνήμης που ονομάζεται TrustZone-protected Memory**(εικόνα_20)**, προτού να δώσει επιβεβαίωση για να προχωρήσει η διαδικασία στο επόμενο**.** Τα hashes που υπολογίζονται είναι για τους έναν ή παραπάνω secondary bootloaders, τον application bootloader του λειτουργικού και του kernel του Normal World. Τα Hashes αυτά, χρησιμοποιούνται για την πιστοποίηση της ακεραιότητας του συστήματος σε δεύτερο χρόνο, μετά δηλαδή το πέρας της διαδικασία της εκκίνησης μέσω της διαδικασίας **TIMA Attestation**.



Εικόνα 20 Διαδικασία Trusted Boot, by Samsung Knox-Security Solution whitepaper

Εάν έχει υπάρξει παρέμβαση σε low-level επίπεδο, σε bootloader, θα βγει μήνυμα στην οθόνη να πάμε τη συσκευή στο πλησιέστερο service. Εάν έχει υπάρξει παρέμβαση στον Kernel (βλέπε rooting), τότε ενεργοποιείται η ασφάλεια Knox Warranty που αναφέραμε παραπάνω. Αυτό θα σημαίνει πως χαρακτηριστικά του Samsung Knox δεν θα είναι διαθέσιμα. Και δεν θα δουλεύει και το Samsung Pay καθώς η συσκευή θα φαίνεται ως πειραγμένη.

Rollback Prevention (RP), όπου απαγορεύεται να φορτωθεί μια πιστοποιημένη αλλά απαρχαιωμένη έκδοση τμημάτων εκκίνησης, καθώς είναι πολύ πιθανό να είναι εκτεθειμένα σε αδυναμίες και προβλήματα που έχουν ανακαλυφθεί και ξεπεραστεί με updated εκδόσεις τους. Η ελάχιστα αποδεκτή έκδοση του Bootloader είναι περασμένη σε μία ασφαλή hardware ασφάλεια ενώ η αντίστοιχα ελάχιστα αποδεκτή έκδοση του Kernel βρίσκεται αποθηκευμένη στον ίδιο τον Bootloader.Οι εκδόσεις αλλάζουν μόνο σε συγκεκριμένα updates και μόνο προς τα πάνω (κάθε φορά δηλαδή έχουμε όλο και πιο «καινούργιες» εκδόσεις που δεν γίνονται δεκτές). Εάν εντοπιστεί έκδοση μη αποδεκτή, τότε το αντίστοιχο process κόβεται και σταματά η διαδικασία φόρτωσης.

Με την δικλείδα ασφαλείας ότι έχουν τρέξει οι Bootloaders σε Trust-Zone περιβάλλον, έχουμε δύο services ασφάλειας που τρέχουν στο Knox.

1. **CCM (Client Certificate Management)**, ενεργοποιείται μόλις κατέβει η ασφάλεια Knox Warranty σε περίπτωση παρέμβασης στο σύστημα. Παρέχει στο σύστημα ένα PKCS#11 interface(public key cryptographic standard (50)), το οποίο επιτρέπει της προσομοίωση μιας smartcard, επιτρέποντας στο TIMA CCM να μοιράζει και να αποσύρει ψηφιακά πιστοποιητικά. Τα πιστοποιητικά και τα παρεμφερή κλειδιά τους είναι κρυπτογραφημένα με μοναδικό για την συσκευή κλειδί. (FIPS-140 2 compliant (51)**)**
2. **(TIMA) Keystore**, είναι μία υπηρεσία, επίσης Trust-Zone based, η οποία παρέχει στις εφαρμογές την δυνατότητα να δημιουργούν και να κρατάνε για λογαριασμό τους κρυπτογραφικά κλειδιά. Τα κλειδιά αυτά κρυπτογραφούνται εκ νέου με το device-specific κλειδί **DUHK** όπως αναφέρθηκε παραπάνω και κατά συνέπεια αποκρυπτογραφούνται μόνο από αυτό. Εάν υπάρξει παρέμβαση στο σύστημα όπως έχει οριστεί στο Trust-Boot, το service αυτό και οι κρυπτογραφικές υπηρεσίες που προσφέρει παγώνουν.

Στηριζόμενο στη ασφαλή βάση που παρέχει το Trust-Boot, το συνεχές Monitoring και τα Services που παρέχουν ασφαλή πιστοποιητικά και κρυπτογραφικά κλειδιά, έρχεται το Application level και το κομμάτι που ονομάζεται Knox Workspace. Το Knox Workspace επιτρέπει, σε εταιρικό περιβάλλον τον διαχωρισμό των εφαρμογών και δεδομένων της συσκευής σε δύο διαφορετικά περιβάλλοντα (κόσμους αν λάβουμε υπόψη την ορολογία του Arm Trustzone). Σε επίπεδο ενός απλού χρήστη, μπορεί να ξεχωρίσει απλά δεδομένα και εφαρμογές με αυτά που στηρίζονται σε ευαίσθητα ή προσωπικά δεδομένα, στηριζόμενο στην πλατφόρμα ασφάλειας που παρέχει το Knox όπως αναφέρθηκε πριν.

Το Workspace δύναται να παρέχει πλήρες ξεχωριστό περιβάλλον, με Home screen, launcher, εφαρμογές και widgets. Εφαρμογές, δεδομένα και αρχεία εκτός Workspace δεν επηρεάζουν ότι είναι εντός. Εάν για παράδειγμα, ετοιμάσω ένα αρχείο κειμένου με εφαρμογή εντός του Workspace, δεν θα μπορώ να το δω έξω από αυτό, ούτε θα μπορώ να το κάνω copy/paste.

Το Workspace χρησιμοποιεί two-factor authentication, επιλέγοντας δακτυλικό αποτύπωμα ως πρώτο βήμα και ανάμεσα σε pin, password ή pattern ως δεύτερο. Σημαντικό στοιχείο πάνω στο πλαίσιο της εργασίας, στην τελευταία έκδοση του Workspace επιτρέπεται η λειτουργία του Bluetooth και του NFC. Το NFC επιτρέπει στη συσκευή να λειτουργήσει με Smartcard-based πιστοποίηση για περιπτώσεις ελέγχου εισόδου ή για είσοδο σε κάποιο λογαριασμό.

Το Knox, διαχωρίζει τα δεδομένα σε προστατευμένα και ευαίσθητα. Όσα δεδομένα γράφονται από εφαρμογές στο secure Workspace θεωρούνται προστατευμένα (52), είναι κρυπτογραφημένα στον δίσκο από το **TIMA Keystore**, οπότε δεν μπορούν να αποκρυπτογραφηθούν έξω από την συσκευή.

Τα ευαίσθητα δεδομένα λαμβάνου επιπλέον προστασία. Στο περιβάλλον του Knox, ως ευαίσθητα δεδομένα κατηγοριοποιούνται όσα βρίσκονται μέσα σε ένα επιλεγμένο Directory εντός του Knox Chamber το οποίο ονομάζεται Chamber. Τα δεδομένα που μπαίνουν εκεί και μαρκάρονται ως ευαίσθητα, προστατεύονται από το SDP (sensitive data protection) το οποίο δημιουργεί ένα container master key και ξεκλειδώνει μόνο με user input. Κάθε φορά που κλειδώνει η συσκευή, διαγράφει όλα τα κλειδιά από την μνήμη και ότι υπάρχει στην cache του Kernel του λειτουργικού.

6.6. Συμπεράσματα για την Λειτουργία του Samsung Pay

Δεν έχει γίνει καμία ξεκάθαρη παρουσίαση ή white-paper για το πλήρες μοντέλο λειτουργίας του. Συλλέγοντας πληροφορίες και παρατηρώντας το παραπάνω μοντέλο ασφάλειας των νέων android συσκευών, προκύπτουν κάποια ασφαλή συμπεράσματα και κάποιες εικασίες.

- Στηρίζεται τόσο σε NFC όσο και Magstripe κάρτα, που σημαίνει ότι είναι εκτεθειμένο στα προβλήματα που είχαν οι κάρτες μαγνητικής ταινίας.
- Δουλεύει τόσο με HCE όσο και SE, χωρίς να ξεχωρίζει τον τρόπο που υλοποιείται το καθένα.
- Η εφαρμογή Samsung Pay, πιθανόν να τρέχει ως service μέσα στο Chamber του Samsung Knox.
- Κατά την διαδικασία πιστοποίησης της κάρτας για χρήση στο Samsung Pay από την εκδότρια τράπεζα, θα μπορούσε να γίνεται κάποιο request για Hardware Attestation,

ελέγχοντας ένα παράγωγο του κλειδιού DUHK και διάφορες μετρήσεις από το Trusted Boot (για παράδειγμα το Warranty bit) και εάν υπάρχει υποψία για exploitation της συσκευής, δεν προχωρά η επικύρωση της κάρτας.

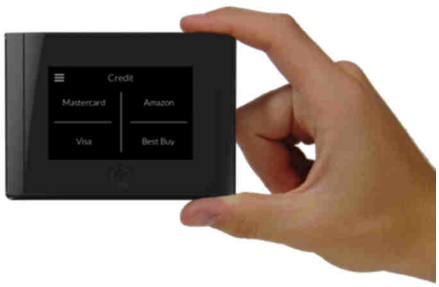
- Αντίστοιχα, θα μπορούσε να μην γίνει δεκτή μία πληρωμή, ύστερα από αποτυχία στον έλεγχο του integrity μιας συσκευής μέσω Hardware Attestation.

7. WOCKET

7.1. Εισαγωγή

Το Wocket είναι η μοναδική υλοποίηση που παρουσιάζεται στην εργασία η οποία δεν αποτελεί εφαρμογή κάποιας τηλεφωνικής συσκευής, αλλά μία αυτόνομη ηλεκτρονική συσκευή με ρόλο Smart Wallet. Είναι προϊόν της NXT-ID, μια εταιρία η οποία δραστηριοποιείται στον τομέα των βιομετρικών εφαρμογών. Προσφέρει την δυνατότητα να κρατάει όλες τις κάρτες αποθηκευμένες ηλεκτρονικά σε ένα secure vault εντός της συσκευής και την χρήση τους μέσω μόνο του Wocket, χωρίς να είναι απαραίτητη η σύνδεση μας στο Internet. Προσφέρει authentication μέσω pin αλλά και μέσω voice recognition.

Στην συσκευασία του Wocket, βρίσκει κανείς τρία βασικά εξαρτήματα, την κύρια συσκευή η οποία αποθηκεύει τις κάρτες, μία “soft” ηλεκτρονική κάρτα (μεγέθους κανονικής τραπεζικής κάρτας) η οποία διαθέτει στην πίσω μεριά της μια μαγνητική ταινία (dynamic mag strip) και ένα card reader**(εικόνα_21)**. Για να περαστούν τα στοιχεία των καρτών στο Wocket, συνδέεται ο card reader στη συσκευή, περνάει την κάρτα από μέσα, επιβεβαιώνεται μέσω ενός 2^{ου} swipe, συμπληρώνεται manually στοιχεία όπως το όνομα που θα φαίνεται ή κάρτα και το CVV και είναι έτοιμη. Μπορεί να αποθηκεύσει τα δεδομένα έως και 10 χιλιάδων καρτών περιλαμβανομένων debit, credit, loyalty/membership. Υποστηρίζει Barcode και QR code, τα οποία είναι αναγνώσιμα από την e-paper lcd οθόνη του.



Εικόνα 21 Ψηφιακό Πορτοφόλι Wocket, by Wocket Gallery

Οι συναλλαγές γίνονται μέσα από την δική του soft κάρτα. Έχοντας την κάρτα μέσα στη συσκευή, ο cardholder επιλέγει από το μενού της συσκευής την κάρτα που θέλει να χρησιμοποιήσει. Αφού ζητηθεί authentication είτε με PIN είτε με Voice recognition, τα στοιχεία που επέλεξε, περνάνε στην κάρτα του Wocket την οποία και μπορεί πλέον να χρησιμοποιήσει σαν να ήταν κανονική κάρτα Mag-stripe. Δεν απαιτείται κάποια εφαρμογή ή σύνδεση με Internet. Για την περίπτωση που χρειάζεται επιβεβαίωση για την συναλλαγή με το CVV ή τα τελευταία 4 ψηφία της κάρτας, αυτά φαίνονται στην πίσω μεριά σε μια μικρή ένδειξη κάτω αριστερά.

Το Wocket θα υποστηρίζει μελλοντικά πληρωμές μέσω Bluetooth και EMV καρτών μέσω NFC και συνεργασία με application από smartphone, καθώς η συσκευή από μόνη της δεν διαθέτει αυτή τη δυνατότητα (53) Επιπλέον, θα υποστηρίξει και πληρωμές από crypto-currency πλατφόρμες, όπως BitCoin, επιτρέποντας με μία μέθοδο να συγχρονίζονται hashes από blockchains για συναλλαγές και επιβεβαίωση υπολοίπου λογαριασμού (για να μην έχουμε double payments). Έτσι, θα προσπαθήσουν να κάνουν δυνατή την χρήση των crypto-currency, τόσο σε online όσο και σε Brick & Mortar συναλλαγές, κάνοντας χρήση συμβατικών φυσικών μέσων πληρωμής (POS).

Σε αντίθεση με τις υπόλοιπες mobile wallet υλοποιήσεις, το Wocket δεν χρειάζεται την συνδρομή εταιριών παροχής κινητής τηλεφωνίας ούτε κάποια ιδιαίτερη συμφωνία με τους τραπεζικούς οργανισμούς. Θα πρέπει όμως να βρει λύση στην χρήση καρτών EMV χωρίς να χρειάζεται την συνδρομή κινητού τηλεφώνου για να τα φέρει εις πέρας

7.2. Ασφάλεια του Wocket

Το Wocket, όπως αναφέρθηκε, υποστηρίζει εκτός από Pin και Voice authentication. Είναι text-dependent που σημαίνει ότι αναγνωρίζει τόσο το δείγμα φωνής όσο και το κείμενο. Αυτό από μόνο του επιτρέπει ένα είδος two-factor authentication (54)**.** Ο αλγόριθμος που χρησιμοποιείται για την διαδικασία του authentication ονομάζεται MobileBio Voice match. Στο μέλλον η συσκευή θα προσφέρει την δυνατότητα και επιπλέον μεθόδων βιομετρικής ταυτοποίησης όπως για παράδειγμα facematch και fingerprint, αλλά και **Behavioral-Directed**, όπου θα μπορεί να περιλαμβάνει εκφράσεις προσώπου, κινήσεις χεριού, drawn pattern, pin (γενικά οτιδήποτε μπορεί να ανιχνευθεί από κίνηση/ήχο και να συνδυάσει έτσι κάτι μοναδικό για το άτομο όπως βιομετρικό με μια μοναδική συμπεριφορά όπως η κίνηση).

7.3. Συμπεράσματα για το Wocket

Προσφέρει ακριβώς τον ορισμό ενός smart wallet, χωρίς να εκθέτει τον user στους κινδύνους που έχει το περιβάλλον του cloud και του λειτουργικού των κινητών τηλεφώνων. Δεν προσπαθεί να ελκύσει τον χρήστη να χρησιμοποιήσει ένα διαφορετικό μοντέλο πληρωμών, για παράδειγμα χρησιμοποιώντας το κινητό, οπότε είναι πιο εύκολο να μπει στην κουλτούρα ενός καταναλωτή. Κυκλοφορεί με αξεσουάρ στα οποία θα μπορεί να μπουν κάρτες όπως δίπλωμα οδήγησης και ταυτότητα (σε χώρες όπου τα παραπάνω έρχονται σε κάρτες με Magstripe τα στοιχεία των δημοσίων αυτών εγγράφων/καρτών μπορούν να περαστούν επίσης στο Wocket) ακόμα και μετρητά οπότε δίνει μια ολοκληρωμένη εικόνα πορτοφολιού νέας εποχής το οποίο μας απαλλάσσει από τις πολλές κάρτες.

Έχει όμως ακόμα να διανύσει πολύ δρόμο καθώς αρκετές από τις δυνατότητες του είναι ακόμα σε εξέλιξη. Τα βιομετρικά του μέτρα προστασίας δεν έχουν ενεργοποιηθεί ακόμα, ενώ εξαρτάται από κινητό τηλέφωνο με εγκατεστημένο το MyWocket app για να δουλέψει με EMV κάρτες μέσω NFC.

8. Android Pay

8.1. Εισαγωγή-Google Wallet

Η Google ήταν η πρώτη εταιρία που εισήγαγε την έννοια του mobile wallet στην αγορά, με την παρουσίαση του Google Wallet. Η εφαρμογή λανσαρίστηκε το 2011 με κύριο κοινό τα android κινητά κάνοντας χρήση του προτύπου NFC για επικοινωνία με τα τερματικά. Αντιμετώπισε μεγάλο ανταγωνισμό τόσο από τους retailers, με εταιρίες μεγέθους όπως η Target και Walmart να λανσάρουν το δικό τους σύστημα πληρωμής (CurrentC) παροπλίζοντας παράλληλα το NFC στα καταστήματα τους, αλλά δυσκολεύτηκε και από τους πάροχους τηλεφωνίας, όπως έγινε για παράδειγμα έγινε με την Softcard (πρώην Isis) η οποία αποτέλεσε μια κοινή συνεργασία μεταξύ των AT7T, T-Mobile και Verizon, η οποία πρόσφερε την δική της mobile πλατφόρμα πληρωμών μέσω NFC. Είναι αρκετά ειρωνικό βέβαια το γεγονός ότι το μεγαλύτερο ποσοστό της Softcard τελικά εξαγοράστηκε από την Google.

Πέρα όμως από τον ανταγωνισμό, η πλατφόρμα του Google Wallet παρουσίασε και αρκετά προβλήματα τεχνικής φύσης. Σε αντίθεση με τους σημερινούς ανταγωνιστές, δεν χρησιμοποίησε tokenization και τα γηγενή προβλήματα ασφάλειας του Android και το γεγονός πως η εφαρμογή λειτουργούσε ελεύθερα σε **rooted** συσκευή, έφερναν στο φως συνεχή κρούσματα ασφάλειας. Συνοπτικά αναφέρονται τα πιο σημαντικά που βρέθηκαν από την ημέρα της εμφάνισης και λειτουργίας του.

1. Relay επίθεση, όπου χρησιμοποιώντας ένα Trojan relay software, λάμβανε εντολές πληρωμής over the air (**OTA**) μέσω ενός relay server και χρησιμοποιούσε τα credential μέσω του secure element της Google για live πληρωμές (55)**.**
2. Το google wallet ήταν συνδεμένο με την συσκευή και όχι κάποιο google account, οπότε ο οποιοσδήποτε κατάφερνε να ανοίξει τη συσκευή, έμπαινε στην εφαρμογή του Wallet έκανε reset, και όταν την άνοιγε πάλι του ζήταγε να δηλώσει εκ νέου στοιχεία όπως Pin, αλλά είχε κρατήσει τα στοιχεία για τις google prepaid κάρτες που πιθανόν να είχε μέσα (fixes in ver. 1.1-R41v8).
3. Αρκετά δεδομένα ήταν αποθηκευμένα σε SQLite Databases, όπως υπόλοιπα λογαριασμών, τραπεζικά όρια ανάληψης, ημερομηνίες λήξης καρτών, ονόματα καρτών κα.

4. Το όνομα της κάρτας, ημερομηνία λήξης, τελευταία 4 ψηφία και λογαριασμός email, ήταν recoverable.
5. Η εφαρμογή κρατούσε μία recoverable εικόνα της κάρτας η οποία έδινε πάλι τα ημερομηνία λήξης, τελευταία 4 ψηφία και όνομα (56) (fixed in version 1.0-R33v6).

Όλα τα παραπάνω οδήγησαν την ανάκληση της εφαρμογής ως Mobile Wallet. Σήμερα πλέον, ύστερα από αρκετές αλλαγές, λειτουργεί ως τρόπος ανταλλαγής χρημάτων μεταξύ ιδιωτών (peer to peer), σχεδόν όπως λειτουργούσε αρχικά το PayPal και τώρα τα Venmo και Square Cash.

8.2. Κυκλοφορία του Android Pay

Η Google λοιπόν, μετά και την εξαγορά της Android, προχώρησε στο επόμενο βήμα της στην αγορά των Mobile Wallets, λανσάροντας το **Android Pay** τον Σεπτέμβρη του 2015. Η υπηρεσία προσφέρεται για την ώρα μόνο στην Αμερική(με άμεσα σχέδια να εμφανιστεί και στην Αυστραλία στο 1^{ο} μισό του 2016, έχει συνεργασία με τα Payment networks των Visa, Mastercard, Discover και American Express, ενώ υποστηρίζεται από 12 μεγάλες τράπεζες όπως Citi, US Bank, American Express και Bank of America (57)**.** Μπορεί να πληρώσει κανείς σε πάνω από 50 αλυσίδες καταστημάτων instore (όσα δηλαδή είναι NFC compatible), ενώ πλέον υποστηρίζονται και συναλλαγές από εφαρμογές.

Το Android Pay μπορεί να λειτουργήσει σε συσκευές με έκδοση Android Kit Kat (4.4 και άνω). Η η συσκευή θα πρέπει να υποστηρίζει **NFC** και **HCE** καθώς σε αντίθεση με την Apple, η αποθήκευση του token **δεν** γίνεται στο secure element της συσκευής, αλλά στο Cloud. Για να γίνει προσθήκη μια κάρτας ο cardholder ανοίγει την εφαρμογή, επιλέγει “Add a credit or Debit Card” και χρησιμοποιώντας την κάμερα του κινητού εισάγει τα στοιχεία ή τα προσθέτει manually. Ο πραγματικός αριθμός της κάρτας του, δεν αποθηκεύεται ποτέ, αλλά στην θέση του εμφανίζεται ένας virtual αριθμός ο οποίος και χρησιμοποιήται για τις συναλλαγές. Στην περίπτωση επιστροφής, χρησιμοποιεί τα τελευταία 4 ψηφία του virtual αυτού αριθμού κάρτας. Ως default κάρτα πληρωμών είναι αυτή που έχει δηλωθεί πρώτη, αλλά αλλάζει εύκολα από την home screen όπου διαλέγει την κάρτα του και επιλέγει “set as default”. Για να αλλάξει στοιχεία όπως ημερομηνία λήξης, κάνω “sign in” στο Payment Methods του Google Account του. Δεκτές γίνονται κάρτες σύμφωνα με τις συνεργασίες που έχει μέχρι στιγμής η Google. Όπως και στις εφαρμογές της Samsung & Apple, σε περίπτωση που υπάρξει απώλεια της συσκευής, μπορεί να

την καλέσει ή να ζητήσει κλείδωμα ή/και διαγραφή των στοιχείων της, μέσα από το Android Device Manager που μπορεί να βρει μέσα από το google account του.

Για να προχωρήσει μία πληρωμή χρειάζεται μόνο να φέρει την συσκευή του πάνω από το NFC enabled τερματικό POS και να χρησιμοποιήσει το δακτυλικό του αποτύπωμα ή το PIN του, αλλά μόνο εάν αυτό του ζητηθεί(εξηγείται παρακάτω). Αντίστοιχα, εάν θέλει να πληρώσει μέσα από μια εφαρμογή καταστήματος, επιλέγει το σήμα "Android Pay" και προχωράει σε online πληρωμή επιλέγοντας την κάρτα που θα χρησιμοποιήσει.

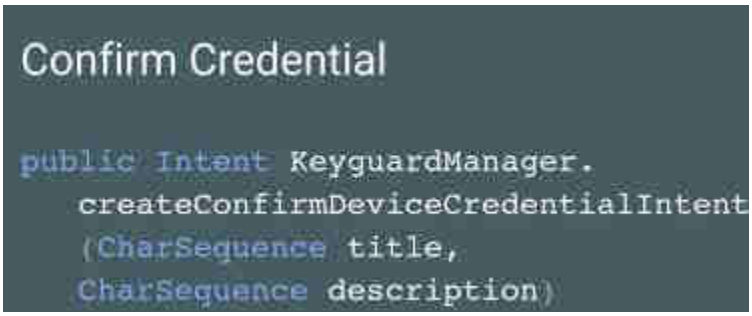
8.3. Μοντέλο Ασφάλειας του Android Pay (Basics)

Το λειτουργικό Android, στη νέα του έκδοση, Android 6.0 (Marshmallow), δίνει την δυνατότητα για authentication μέσω fingerprint για όσες συσκευές διαθέτουν fingerprint scanner. Έτσι, είναι δυνατόν να ξεκλειδώνεται η συσκευή αλλά και να επικυρώνονται συναλλαγές μέσω Android Pay. Το Android Pay API έχει υλοποιηθεί έτσι ώστε η κάθε εταιρία να μπορεί να ενσωματώνει στα δικά της apps πληρωμών την δυνατότητα πληρωμής μέσω Android Pay. Σημαντικό ρόλο στο authentication της διαδικασίας πληρωμής, αλλά και στο σύνολο της ασφαλής λειτουργίας των εφαρμογών, έχουν τα εξής δύο API, το **Fingerprint API** και το **Confirm Credential API**.

- **Fingerprint API**, χρησιμοποιώντας το (νέο) **Fingerprint Manager class**, Μπορεί να κάνει αγορές σε apps δίνοντας confirmation με το δακτυλικό αποτύπωμα. Το API **(εικόνα_22)** επιτρέπει στην εφαρμογή να κάνει authenticate τον cardholder με το δακτυλικό αποτύπωμα. Το App, λαμβάνει ένα authentication callback από τον αισθητήρα μόλις ανιχνευθεί το αποτύπωμα. Αυτό γίνεται κάθε φορά που το απαιτεί η εφαρμογή. Χρησιμοποιεί Keystore για να δημιουργεί και χρησιμοποιεί cryptographic keys.

Εικόνα 22 Fingerprint API, by Google Developers-Android Pay

- **Confirm Credential API**, με αυτό το API **(εικόνα_23)**, χρησιμοποιεί το user's lock screen, για να κάνει πιστοποίηση του cardholder. Όταν κάνει tap-and-pay για προχωρήσει σε μία αγορά, το App ελέγχει πότε ξεκλειδώθηκε τελευταία φορά το κινητό. Εάν έχουν περάσει πάνω από 5 λεπτά, θα ζητήσει να ξεκλειδωθεί το κινητό μέσω της user's lock screen προτού προχωρήσει. Οπότε, πιστοποίηση δεν ζητάει σε κάθε αγορά και το δακτυλικό αποτύπωμα χρησιμοποιήται μόνο στα Apps. Πέρα από device unlock, κάνει και application unlock. Συνδυάζοντας το user's lock screen μαζί με ένα time-out policy του πότε ήταν η τελευταία φορά που έγινε unlock η συσκευή, η συσκευή κλειδώνει αν μείνει αρκετά ανενεργή. Το κάνει επιτρέποντας στην εφαρμογή να δημιουργήσει ένα κλειδί από ένα key generator και να το αποδώσει στο device lock screen μαζί με ένα time-out policy. (πχ. Πέρασαν 1-2-5 λεπτά/sec από το τελευταίο ξεκλείδωμα). Όταν η εφαρμογή θελήσει να κάνει authenticate τον χρήστη, ξεκινά χρησιμοποιώντας το κρυπτογραφικό κλειδί. Αν αυτό αποτύχει, τότε καλείται να πιστοποιηθεί στην συσκευή μέσω του Confirm Credential API. Αυτό αυτόματα ξεκλειδώνει το κρυπτογραφικό κλειδί. Τα access time-outs των κλειδιών είναι συγχρονισμένα στο σύστημα, όποτε οι διάφορες εφαρμογές ζητάνε authentication όποτε χρειάζεται η κάθε μία ανεξάρτητα από τις άλλες.



Εικόνα 23 Confirm Credential API, by Google Developers-Android Pay

8.4. Μοντέλο Ασφάλειας του Android Pay (Intermediate)

Είτε ο cardholder πρόκειται να πληρώσει μέσω από NFC-enabled POS είτε Online, η Google είναι αυτή που έχει τον ρόλο του TSP και προμηθεύει το token στον merchant. Μόλις ο cardholder πιστοποιήσει τη συναλλαγή, αυτή προωθείται στην Google. Το πακέτο δεδομένων που παραδίδεται στον merchant έχει συνοδεύεται από dynamic cryptogram για την κάθε

συναλλαγή ενώ το token είναι σταθερό. Σύμφωνα με την Risk Engine της Google, το token έχει ένα ρυθμό με τον οποίο γίνεται refresh και δεν κρατάει παραπάνω από ένα χρόνο (3). Από την στιγμή που, προς το παρών, η Google είναι ο μοναδικός TSP για τις υπηρεσίες του Android Pay, διατηρεί το δικαίωμα να δίνει τα τελευταία 4 ψηφία του token στον cardholder και τον merchant, για την περίπτωση που χρειάζεται διευθέτηση διαφορών και διευκρινήσεις. Εδώ να σημειωθεί ότι το παραπάνω γεγονός, ότι είναι δηλαδή ο μοναδικός TSP για την υπηρεσία της, αυτόματα σημαίνει ότι δεν ακολουθεί το process της EMVCo. Παρόλα αυτά, υποστηρίζει το μοντέλο και γίνονται κινήσεις για alignment.

Τα μοντέλα ασφάλειας που χρησιμοποιεί η Google, έχουν μεθόδους που καλύπτουν τόσο τα δεδομένα που μεταδίδονται όσο και αυτά που είναι αποθηκευμένα (data-at-rest). Η Google δίνει περισσότερο βάση στο γεγονός ότι η πληροφορία της συναλλαγής που μεταφέρεται είναι δυναμική, παρά η δυναμική ή σταθερή φύση του token. Χρησιμοποιεί όμως μία ιδιαίτερη Risk Engine η οποία λαμβάνει υπόψη κινήσεις και χαρακτηριστικά του προφίλ του cardholder για να προχωρήσει στο authentication μια συναλλαγής.

8.5. Μοντέλο Ασφάλειας του Android Pay (Advanced)

- Πληρωμή μέσω εφαρμογής

Όπως αναφέρθηκε και προηγουμένως, αντί να προωθείται ο πραγματικός αριθμός της κάρτας στον έμπορο, η Google δημιουργεί ένα Virtual Account Number (VAN), ο οποίος χρησιμοποιήται μόνο για την συγκεκριμένη συναλλαγή για την οποία δημιουργήθηκε. Με αυτό τον λογαριασμό, ο Merchant προωθεί την συναλλαγή στο τραπεζικό δίκτυο. Μόλις ο cardholder επιλέξει προϊόν για αγορά και προχωρήσει σε check-out, στο App του εμπόρου προωθείται ένα κρυπτογραφημένο πακέτο πληροφοριών όπως χώρος παράδοσης και στοιχεία χρέωσης, που ονομάζεται Masked Wallet. Η εφαρμογή της πληρωμής, χρησιμοποιεί Elliptic Curve Public Key για το κομμάτι του Masked Wallet request (58). Μόλις η εφαρμογή του εμπόρου λάβει την πληροφορία του Masked Wallet, επιστρέφει στον χρήστη ένα confirmation page. Μόλις επιβεβαιώσει ο cardholder, η εφαρμογή ζητάει το λεγόμενο **Full Wallet Request**, το οποίο περιλαμβάνει όλες τις πληροφορίες που είχε το Masked Wallet και επιπλέον, το τελικό ποσό πληρωμής (με φόρους πχ).

Το Android Pay χρησιμοποιεί **Elliptic Curve Integrated Encryption Scheme** (ECIES) για την ασφάλεια του token του **Full Wallet Request**, με τις παρακάτω παραμέτρους

1. Η μέθοδος για Key encapsulation είναι η ECIES-KEM, όπως ορίζεται στο ISO 18033 με χρήση Elliptic curve κατά NIST P-256
2. Key Derivation Function με HKDF with SHA256, χωρίς salt και 128 bits πληροφορίας για το AES128 key και άλλα 128 bits για το HMAC_SHA256 key
3. Για τον αλγόριθμο συμμετρικής κρυπτογράφησης, χρησιμοποιήται DEM2("οικογένεια" μηχανισμών data encapsulation (59) σύμφωνα με το ISO 18033-2 με τις παρακάτω παραμέτρους:
    - encryption algorithm: AES128 CTR with zero IV and no padding
    - Mac algorithm: HMAC_SHA256 χρησιμοποιώντας το κλειδί των 128bits από το 2^{ο} βήμα.

Αντίστοιχα για την αποκρυπτογράφηση του Token, χρησιμοποιείται το παρακάτω:

1. Χρησιμοποιώντας το ιδιωτικό κλειδί και το Public Key που δημιουργήθηκε για το session (ephemeral), προκύπτει ένα 256 bit shared key χρησιμοποιώντας ECIES-KEM, σύμφωνα με το ISO 18033-2, με τα παρακάτω στοιχεία:
    - Elliptic curve, μέσω NIST P-256
    - Key Derivation Function: HKDFwithSHA256, χωρίς salt και η πληροφορία σε encoded σε ASCII
2. Χωρίζει το κλειδί των 256-bit που έχει δημιουργηθεί σε 2 των 128-bit,
3. Για την δημιουργία του MAC, χρησιμοποιεί HMAC με SHA256 και το ένα από τα 2 κλειδιά των 128-bit από το βήμα 2.
4. Αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας AES128 CTR mode με zero IV, χωρίς padding, και το 2^{ο} από τα 2 128-bit κλειδιά του 2^{ου} βήματος.

8.6. Συμπεράσματα.

Τα παραπάνω αποτελούν οδηγίες προς τους vendors των κινητών και τις εταιρίες που θα ετοιμάσουν τις online εφαρμογές των εμπόρων. Δεν υπάρχει εγγύηση για την ασφάλεια του τελικού αποτελέσματος. Ακόμα και εάν το αποτέλεσμα είναι εγγυημένο για μία έκδοση του Android, δεν ξέρουμε τι μπορεί να συμβαίνει με τις προηγούμενες και όλα τα προβλήματα που παρουσίασαν.

Σε hardware επίπεδο, δεν είναι γνωστό το κατά πόσο ο επεξεργαστής διαθέτει TrustZone όπως οι τελευταίας γενιάς επεξεργαστές των Samsung συσκευών.

Σε software επίπεδο, βρέθηκαν και εδώ προβλήματα, Με εφαρμογές που είχαν από τη φύση τους privileged δικαιώματα, όπως remote support tools (**mRSTs**) (60) όπως το TeamViewer. Αυτές χρειάζονται δικαιώματα για να με αφήσουν να κάνω Login στη συσκευή ή να κάνω picture capture, ή simulation σε user input, αλλά είναι του ίδιου τύπου δικαιώματα που ζητάνε κακόβουλο λογισμικό τύπου mobile remote access Trojans (**mRATs**). Πολλές συσκευές είχαν/έχουν τέτοιες εφαρμογές προ-εγκατεστημένες ή έστω ένα low-level service plugin.

9. Συμπεράσματα

Οι υλοποιήσεις των mobile wallets που παρουσιάστηκαν παραπάνω, έχουν κάποια κοινά χαρακτηριστικά αλλά κάποια στοιχεία που διαφοροποιούνται. Ακολουθεί μία συνοπτική κατάθεση των στοιχείων εκείνων που έχουν και την μεγαλύτερη βαρύτητα στο κομμάτι της ασφαλής χρήσης τους.

9.1. Μοντέλο Επικοινωνίας

Στο πλαίσιο της επικοινωνίας της συσκευής με τον έμπορο, το NFC πρωτοστατεί. Προσφέρει embedded προστασία μέσω AES κρυπτογράφησης και έχει πολύ μικρό φάσμα επικοινωνίας οπότε και κάνει πολύ δύσκολη την υποκλοπή των δεδομένων κατά την μετάδοση τους στο POS τερματικό (ο επιτιθέμενος θα πρέπει να είναι πολύ κοντά ή θα πρέπει να έχει εκτεθεί σε επίθεση το ίδιο το POS από κάποιο Malware). Το μοντέλο mag-stripe θεωρείται πλέον ξεπερασμένο και με πολλά προβλήματα. Για το λόγο αυτό και αρκετοί τραπεζικοί όμιλοι ενώ υιοθετούν το Wallet της Samsung, αποφασίζουν να μην υποστηρίξουν το MST χαρακτηριστικό, όπως για παράδειγμα πράττει η CaixaBank. Το Wocket σε αυτό τον τομέα θα πρέπει να κινηθεί γρήγορα στην υλοποίηση της Bluetooth υποστήριξης, αν και πάλι θα κληθεί να αντιμετωπίσει τα εξής προβλήματα λόγω.

1. το αυξημένου εύρους επικοινωνίας που έχει (φτάνει τα μερικά μέτρα) σε σχέση με το NFC, οπότε θα πρέπει να περιοριστεί η απόσταση επικοινωνίας μεταξύ των συσκευών
2. να παραληφθεί το χαρακτηριστικό του Multicasting που έχει από την φύση του το Bluetooth, καθώς προσφέρει την δυνατότητα σε μία συσκευή να συνδεθεί παράλληλα με παραπάνω από μία συσκευές.

Αυτές οι κινήσεις φυσικά, περιορίζουν τα φυσικά χαρακτηριστικά του Bluetooth Που το δίνουν πλεονέκτημα σαν πρωτόκολλο επικοινωνίας, οπότε θα ήταν μάλλον πιο αποδοτικό να προσανατολιστούν σε μια NFC υλοποίηση.

9.2. Αποθήκευση Δεδομένων

Εδώ υπάρχουν δύο κυρίαρχα πρότυπα. Οι hardware/software υλοποιήσεις όπου τα ευαίσθητα δεδομένα(αριθμός κάρτας-token, pin, βιομετρικά χαρακτηριστικά) αποθηκεύονται σε ένα SE εντός της συσκευής και οι cloud/software υλοποιήσεις όπου τα ευαίσθητα δεδομένα βρίσκονται σε cloud servers και διαχειρίζονται από τους αντίστοιχους προμηθευτές.

Τόσο η Apple όσο και η Samsung, πραγματοποίησαν μια υλοποίηση δύο “κόσμων”. Ενός περιβάλλοντος για τις τυπικές λειτουργίες της συσκευής και ενός για όσες έχουν εφαρμογές οι οποίες απαιτούν διαχείριση ευαίσθητων δεδομένων, όπως είναι τα Wallets. Η Apple ανέπτυξε τον συνδυασμό ενός SE μαζί με το Secure Enclave (δικό του boot, κλειδιά, κρυπτογράφηση και αποθήκευση του δακτυλικού αποτυπώματος), ενώ η Samsung παρουσίασε την νέα εκδοχή του Knox, βασισμένο πάνω στο Arm TrustZone. Θεωρείται ασφαλές συμπέρασμα πως μέσα στο Chamber θα τρέχει το service του Samsung Pay και το Hardware Attestation προφίλ θα είναι υπεύθυνο για την “ζωντανή” παρακολούθηση της ακεραιότητας της συσκευής. Η Google με την σειρά της προτίμησε το HCE μοντέλο με το βάρος να πέφτει στους Cloud providers. Η υλοποίηση αυτή, λύνει μεν τα χέρια των τραπεζών ως προς το πώς θα ήθελαν να διαχειρίζονται τις εφαρμογές πληρωμής, αλλά τα μοντέλα διαχείρισης τους έχουν ακόμα μικρό βαθμό ωριμότητας και πολύ χαμηλότερο επίπεδο πιστοποίησης σε σχέση με τα hardware SE. Το μέγεθος δε της ζημιάς που μπορεί να προκύψει σε περίπτωση ρήγματος ασφάλειας και διαρροής δεδομένων από έναν cloud server ο οποίος για παράδειγμα διαχειρίζεται δεδομένα καρτών, είναι απείρως μεγαλύτερο από ένα πρόβλημα ασφάλειας που μπορεί να επηρεάσει μια σειρά προϊόντων, καθώς ο αριθμός των συσκευών είναι μεν εν δυνάμει μεγάλος αλλά οι hardware επιθέσεις δεν μπορούν να είναι απόλυτα ενορχηστρωμένες σε συγκεκριμένες συσκευές σε μεγάλη κλίμακα. Το Wocket, λόγω της κάρτας που χρησιμοποιεί, δεν προσφέρει τίποτα καινούργιο στο κομμάτι της διαχείρισης των δεδομένων, καθώς συμπεριφέρεται σαν μια τυπική κάρτα.

9.3. Tokenization

Πάνω στο tokenization, η Apple διαθέτει ίσως το πιο ολοκληρωμένο μοντέλο. Στηρίζεται στο EMVCo πρότυπο, καθώς διατηρεί το σταθερό νούμερο DAN, ως αντικαταστάτη του PAN,μέσα στο SE και το συνδυάζει ανά συναλλαγή με το AR (μη σταθερό ανά συνθήκες) και ένα nonce. Η Samsung λειτουργεί με παρόμοιο τρόπο και κατά το EMVCo πρότυπο. Η Google είναι, μέχρι στιγμής, ο μοναδικός TSP για τις υπηρεσίες της, οπότε και δεν συμμορφώνεται με το EMVCo πρότυπο. Για να περιορίσει το ρίσκο από αυτή την διαφοροποίηση της, επιλέγει να αλλάζει κατά διαστήματα το Token της κάρτας στηριζόμενη στα αποτελέσματα που προκύπτουν από την risk engine που διαθέτει. Το Wocket και πάλι, δεν χρησιμοποιεί κάποιο token και ο αριθμός της κάρτας χρησιμοποιήται αυτούσιος, οπότε και λειτουργεί με τον ίδιο ακριβώς τραπεζικό μηχανισμό που λειτουργεί και μια mag-stripe κάρτα.

9.4. Αυθεντικοποίηση

Ο δρόμος που ακολουθούν όλες οι λύσεις που παρουσιάστηκαν στην εργασία, είναι κοινός και είναι τα βιομετρικά. Το PIN παραμένει σαν δικλείδα ασφάλειας και ως δευτερεύουσα λύση αλλά η κύρια υλοποίηση είναι η χρήση βιομετρικού και κατά κύριο λόγω του δακτυλικού αποτυπώματος. Η Google και η Samsung το προσφέρουν σε συγκεκριμένες συσκευές και εκδόσεις λειτουργικού και πάνω. Η Wocket κάνει μια ευχάριστη έκπληξη καθώς ως εταιρία έχει εξαιρετικό βιογραφικό σε βιομετρικές υλοποιήσεις. Προσφέρει αυθεντικοποίηση μέσω φωνής ενώ μελλοντικά θα φέρει και επιπλέον λύσεις στο προσκήνιο όπως αναγνώριση προσώπου.

9.5. Αποδοχή καρτών

Η μεθοδολογία που χρησιμοποιούν οι υλοποιήσεις mobile wallet που στηρίζονται σε τηλεφωνική συσκευή, για να περάσουν μια τραπεζική κάρτα μέσα στο σύστημα τους παρουσιάζει ελάχιστες διαφορές στο καθαρά τεχνικό κομμάτι. Κυρίως στηρίζονται σε session calls και SSL κρυπτογράφηση για να επικοινωνήσουν με τους τραπεζικούς φορείς. Το σημείο που παρουσιάζει το μεγαλύτερο ενδιαφέρον είναι το αν και πως οι τράπεζες κάνουν δεκτές τις κάρτες. Όπως αναφέρθηκε και πριν, το Yellow Path θα έπρεπε να αποτελεί την προεπιλογή για την αυθεντικοποίηση μιας κάρτας. Οφείλουν δηλαδή οι τράπεζες να θεωρούν ως δεδομένο το έξτρα βήμα αυθεντικοποίησης του card holder ανεξαρτήτως μεθόδου που θα γίνει. Όπως αναφέρθηκε και πριν οι τράπεζες θα πρέπει να ενισχύσουν το μοντέλο διπλής αυθεντικοποίησης και να επικεντρώσουν την προσοχή τους σε άρτια εκπαιδευμένα call centers για την επικοινωνία με τον card holder σε συνδυασμό με αποστολή OTPs.

9.6. Τρόπος Πληρωμής

Στο κομμάτι της πληρωμής, έχουμε αρκετές ομοιότητες αλλά και διαφορές. Η βιομετρική αυθεντικοποίηση αποτελεί την προεπιλογή για την έναρξη της πληρωμής. Η Apple παρουσιάζει το πιο ολοκληρωμένο μοντέλο προστασίας κάνοντας συνδυασμό Hardware(SE & Secure Enclave) και Software(κρυπτογράφηση) στοιχείων αλλά και με μια ιδέα δανεισμένη από Cloud νοοτροπία (επιπλέον nonce, ανά αγορά). Η υλοποίηση της Android κάνει μια μικρή παραχώρηση στο κομμάτι της ασφάλειας για χάρη του user experience, καθώς επιτρέπει συγκεκριμένα time lapses μέσα στα οποία αν πραγματοποιηθεί επιπλέον συναλλαγή, δεν απαιτεί νέα αυθεντικοποίηση του card holder. Η Samsung είναι πολύ πιθανό να έχει συνδέσει τις πληρωμές της με το service του Hardware Attestation, ελέγχοντας την ακεραιότητα της

συσκευής και απαιτώντας ακύρωση της διαδικασίας αν προκύψει ότι υπάρχει θέμα tampering. Στο σενάριο των επιστροφών κάποιων συναλλαγών, παρατηρήθηκε ότι κάθε φορά ζητούνται τα τελευταία 4 ψηφία της κάρτας. Αν και ως κάρτα αναφέρεται η κάρτα token, δεν παύει να δίνει ένα ίχνος πληροφορίας που θα μπορούσε να εκμεταλλευτεί κάποιος για να περιορίσει την τυχαιότητα μια κάρτας. Βάση μοντέλου EMVCo ο αριθμός της κάρτας δεν μπορεί να αλλάζει, οπότε θα πρέπει ίσως να υπάρξει ένα διαφορετικό μοντέλο αυθεντικοποίηση του cardholder.

9.7. Hardware

Η ασφάλεια πλέον δεν στηρίζεται μόνο σε κρυπτογραφία και τεχνικές με γνώμονα την software υλοποίηση. Θα πρέπει να υπάρχει και ισχυρή τεχνική αρχιτεκτονική. Η Apple ως εταιρία είχε δεχθεί πολλές φορές κριτικές για την επιλογή της να είναι εξαιρετικά αυστηρή για το επίπεδο συνεργασίας και επικοινωνίας των συσκευών της με Non-Apple συσκευές, αλλά καθαρά από θέμα ασφάλειας, αυτό ήταν το πιο δυνατό της χαρτί. Είχε πλήρη έλεγχο του hardware της, απέσυρε σε τακτά διαστήματα παλιό εξοπλισμό και σταματούσε την υποστήριξη του, επομένως όποιος ήθελε να επιτεθεί σε συσκευές της έπρεπε κάθε φορά να ξεπεράσει καινούργιες υλοποιήσεις, κάνοντας το ίδιο και τώρα με το Secure Enclave. Η Samsung κινήθηκε εξίσου σωστά, αφήνοντας πίσω τις παλιές συσκευές της, και προχωρώντας σε στιβαρές κατασκευές στηριζόμενες στους καινούργιους επεξεργαστές της ARM με TrustZone αρχιτεκτονική. Η Google δυστυχώς αποφάσισε να υποστηρίξει και παλαιότερα μοντέλα με ότι αυτό συνεπάγεται για παλιά exploits που κυκλοφορούν και καθιστούν επικίνδυνη την χρήση των συγκεκριμένων μοντέλων και συσκευών. Ίσως εδώ η επιλογή της για υποστήριξη του μοντέλου HCE για την αποθήκευση ευαίσθητων δεδομένων να ήταν ιδανική καθώς θα ήταν πρακτικά αδύνατο να βρει λύσεις ασφάλειας για όλα τα παλιά μοντέλα που υποστηρίζει, οπότε το mitigation αυτού το ρίσκου στο Cloud να αποδειχθεί καλή κίνηση.

9.8. Τελικές Σκέψεις

Αν και οι υλοποιήσεις των mobile wallets είναι σχετικά καινούργιες, οι απαιτήσεις που υπάρχουν στον τομέα της ασφάλειας είναι οι ίδιες με αυτές που προσπαθεί να ανταπεξέλθει τα τελευταία χρόνια το τραπεζικό σύστημα. Οι πελάτες δεν αντιλαμβάνονται ακόμα το πόσο κρίσιμος είναι αυτός ο τομέας και υπάρχει ακόμα η αντίληψη ότι αποτελεί τελικά μία τροχοπέδη στην γρηγορότερη εξυπηρέτησή τους. Σε γενικές γραμμές η πλειοψηφία των πελατών δείχνει εξοικειωμένη με την άντληση προσωπικών πληροφοριών καθώς το online banking είχε ήδη

μεγάλη άνθηση. Εδώ ίσως και το σημείο στο οποίο θα πρέπει να στηριχθεί ολόκληρο το οικοσύστημα του mobile wallet/banking για να ενισχύσει την ασφάλεια του. Αν και υπάρχει ήδη ένα γενικότερο ρεύμα προς τα βιομετρικά συστήματα, η λύση ίσως κρύβεται προς το Behavior Analysis. Ήδη μερικές τέτοιες επιλογές εμφανίστηκαν στο Yellow Path βήμα της αποδοχής των καρτών. Θα έχει πλέον σημασία πράγματα όπως οι ώρες που πραγματοποιεί κάποιος μια αγορά, η συχνότητα που αγοράζει, τα ποσά, τα μέρη που δραστηριοποιείται ως καταναλωτής. Θα μπορούσε κάποιος βέβαια να κατηγορήσει, και όχι τόσο άδικα, ότι τίθεται σοβαρό θέμα προστασίας της ιδιωτικότητας. Η ανωνυμία και η μη-συνδεσιμότητα, χαρακτηριστικά τα οποία αποτελούν ολόκληρο κομμάτι μελέτης των Τεχνικών προστασίας της ιδιωτικότητας, θα αποτελούν εμπόδιο σε αυτή την προσέγγιση. Θα υπάρξει, και σωστά, μια σύγκρουση καθώς τα βασικά ερωτήματα που τίθενται στην αυθεντικοποίηση ενός καταναλωτή είναι,

- Τι ξέρει (pin)
- Τι έχει κάρτα
- Ποιος είναι(βιομετρικά)

Οπότε, θα πρέπει να βρεθεί μια σωστή και ισορροπημένη φόρμουλα ώστε να υπάρξει προσωποποίηση της ασφάλειας, θυσιάζοντας όμως όσο το δυνατό λιγότερο πληροφορίες για την ζωή και τις συνήθειες του καταναλωτή. Το μόνο σίγουρο είναι πως η αγορά θα κινηθεί με γρήγορους ρυθμούς προς την προώθηση αυτού του μοντέλου πληρωμών, οπότε είναι χρέος της να εξασφαλίσει την ασφάλεια την συναλλαγών τόσο όσο και την ασφάλεια του καταναλωτή όχι μόνο ως εν δυνάμει αγοραστή αλλά και ως ατόμου και προσωπικότητας.

References

1. **emv-connection. *EMV Migration Forum & Smartcard Alliance.* [Online] May 2015. http://www.emv-connection.com/downloads/2015/05/EMF-Liability-Shift-Document-FINAL5-052715.pdf.**

2. Accepting Visa Cards. *visa.ca.* [Online] 2016. http://www.visa.ca/merchant/accepting-visa-cards/how-visa-payments-work.jsp.

3. Marian Crowe, Susan Pandy, David Lott, Steve Mott. *Is Payment Tokenization Ready for Prime time?* s.l. : Federal Reserve Bank of Atlanta, Federal Reserve bank of Boston, 2015.

4. visa. *Press Release-MasterCard, Visa and American Express Copyright Business Wire.* [Online] 2013. http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1860500.

5. *EMV Payment Tokenisation Specification.* s.l. : EMV, March, 2014.

6. Point, Clear. Credit Card Numbers – What Do They Mean. *Clear Point Credit Counceling Solutions.* [Online] April 11, 2013. http://www.clearpointcreditcounselingsolutions.org/what-do-credit-card-numbers-mean-a-look-at-whats-inside-your-credit-card/.

7. Alliance, Smard card. Smart Card Alliance-Technologies for Payment Fraud Prevention. *EMV-Connection.* [Online] October 2014. http://www.emv-connection.com/downloads/2014/10/EMV-Tokenization-Encryption-WP-FINAL.pdf.

8. Poole, Ian. NFC Tags and Tag Types. *Radio-Electronics.com.* [Online] http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-tags-types.php.

9. developer.android. nearFieldCommunication. *developer.android.* [Online] http://developer.android.com/guide/topics/connectivity/nfc/index.html.

10. Forum, NFC. *NFC Data Exchange Format.* Wakefield, MA, USA : NFC Forum.Inc, 2006.

11. ISO/IEC 14443-1:2008. *iso.org.* [Online] June 15, 2008. http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39693.

12. HP. Bluetooth Wireless Technology Basics. *hp.com.* [Online] 2004. http://www.hp.com/ctg/Manual/c00186949.pdf.

13. Bluetooth SIG, Inc. Bluetooth Core Specification. *Bluetooth.com.* [Online] 2016. https://www.bluetooth.com/specifications/bluetooth-core-specification.

14. Gupta, Naresh. *Inside Bluetooth Low Energy.* Boston, London : Artech House, 2013.

15. Bluetooth, SIG, Inc. Generic Attributes. *Bluetooth.* [Online] 2016. https://www.bluetooth.com/specifications/gatt.

16. Clarke, C.K.P. *R&D White Paper, WHP 031.* UK : BBC , 2002.

17. The History of Fingerprints. [Online] January 9, 2016. http://onin.com/fp/fphistory.html.

18. Fingerprints and Other Biometrics. *FBI.gov.* [Online] https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi.

19. D.Maltoni, D.Maio, A.K Jain, S. Prabhakar. *Handbook of Fingerprint Recognition.* New York : Springer, 2003.

20. Council, National Science and Technology. Speaker Recognition. *FBI.gov.* [Online] https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/speaker-recognition.pdf.

21. Reynolds, Douglas A. *Automatic Speaker Recognition: Current Approaches and Future Trends.* Lexington, USA : MIT Lincoln Laboratory, 2001.

22. Robert J. Elliott, Lakhdar Aggoun, John B. Moore. *Hidden Markov Models, Estimation & Control.* s.l. : Sprienger, 2008.

23. Nuance. Measuring Performance in a Biometrics Based Multi-Factor Authentication Dialog. *Nuance.es.* [Online] 2009. http://www.nuance.es/ucmprod/groups/enterprise/@web/@enus/documents/collateral/nd_006285.pdf.

24. Erika McCallister, Tim Grance, Karen Scarfone. Guide to Protecting the Confidenciality of Personal Identifiable Information. *CSRC.nist.gov.* [Online] April 2010. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

25. N.K Ratha, J.H Connell, R.M Bolle. *Enhancing security and privacy in biometrics-based authentication systems.* s.l. : IBM systems journal, vol 40, 2001.

26. Emilio Bordini, Dimitrios Tzovaras. *Second Generation Biometrics: The Ethical, Legal and Social Context.* s.l. : Springer Netherlands, 2012.

27. *The ABCs of HCE.* Austin : SimplyTapp, October2015.

28. Host-Based card Emulation. *developer_android.* [Online] https://developer.android.com/guide/topics/connectivity/nfc/hce.html.

29. BankofMontreal, CIBC, National Bank of Canada, Royal Bank, Scotiabank, TD Bank Group. *Payments Security White Paper.* 13072015.

30. Symantec. *Internet Security Threat Report.* s.l. : Symantec, 2015.

31. Oscar celestino, Angelo Abendan. Watering Hole 101. *Trend-Micro.* [Online] [Cited: January 3, 2016.] http://www.trendmicro.com.au/vinfo/au/threat-encyclopedia/web-attack/137/watering-hole-101.

32. Arnfield, Robin. *Mobile Payments.* s.l. : Networld Media Group, 2015.

33. Pegeros, Vanessa. *Security of Mobile Banking and Payments.* s.l. : SANS Institute, 2012.

34. Merrit, Cynthia. *Mobile Money Transfer Services: The Next Phase in the Evolution in Person-to-Person Payments.* 2010.

35. Airtime is Money. *The Economist.* [Online] january 19, 2013. http://www.economist.com/news/finance-and-economics/21569744-use-pre-paid-mobile-phone-minutes-currency-airtime-money.

36. Tarek M Mahmoud, Bahgat A. Abdel-latef, Awny A. Ahm. *Hybrid Compression Encryption Technique for Securin.* International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6).

37. mPesa FAQ. *mPesa.* [Online] 2014. https://www.mpesa.in/portal/customer/FAQ.jsp.

38. Bloomeberg Business, Company overview. *Bloomberg.* [Online] http://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=60268423.

39. Apple Support-Apple Pay participating Banks. *Apple Inc.* [Online] December 7, 2015. https://support.apple.com/el-gr/HT204916.

40. iOS Security. *apple.* [Online] September 2015. https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

41. Attridge, Jim. An Overview of Hardware Security Modules. *sans.org.* [Online] January 14, 2002. https://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757.

42. NIST. AES Key Wrap Specification. *csrc.nist.gov.* [Online] November 16, 2001. http://csrc.nist.gov/groups/ST/toolkit/documents/kms/key-wrap.pdf.

43. *Identity Theft and your Social Security Number.* s.l. : Social Security Administration_USA, September,2015.

44. Apple Pay Issue. *passkit.* [Online] July 30, 2015. https://blog.passkit.com/one-major-hsbc-apple-pay-uk-issue-no-one-is-talking-about/.

45. Graylin, William Wang. *#20150363771_US8814046 B1* USA, 17/12/2015.

46. Guillaume Granier, Eric Fohlen-Weill. *Samsungs New Secure Element.* Barchelona : FTI Consulting Strategic Communication, March,2015.

47. The U.S. Department of Defense adds 5 Samsung Galaxy Devices with the KNOX platform to Approved Products List. *samsungmobilepress.* [Online] June 2, 2014. http://www.samsungmobilepress.com/2014/06/02/The-U.S.-Department-of-Defense-adds-5-Samsung-Galaxy-Devices-with-the-KNOX-platform-to-Approved-Products-List-APL-1.

48. Business, Samsung. *Samsung Knox.* [Online] September 2015. https://www.samsungknox.com/en/system/files/whitepaper/files/Samsung%20KNOX%20Security%20Solution_V1.07_0.pdf.

49. TrustZone. *ARM.* [Online] http://www.arm.com/products/processors/technologies/trustzone/index.php.

50. IBM. IBM Knowledge Center, What is PKCS#11. *IBM.* [Online] https://www-01.ibm.com/support/knowledgecenter/linuxonibm/com.ibm.linux.z.lxce/lxce_whatis_pkcs11.html.

51. Standards,FIPS PUB 140-2. *nist-gov.* [Online] November 15, 2001. http://csrc.nist.gov/groups/STM/cmvp/standards.html.

52. Samsung. SamsungKnox. *www.samsungknox.com.* [Online] September 2015. https://www.samsungknox.com/en/system/files/whitepaper/files/An%20Overview%20of%20the%20Samsung%20KNOX%20Platform_V1.12_0.pdf.

53. Charles David Tunnell, Justin Mitchell, Gino Pereira, Jacob Zurasky. *Patent Application, 14/049,175* USA, 2013.

54. NXT-ID's Wocket Smart Wallet with Biometric Security. *bootcamp.* [Online] December 7, 2015. http://www.bootcamp.com/interview.jsp?interviewId=2482.

55. M. Roland, J. Langer, J. Scharinger. *Applying Relay Attacks to Google Wallet.* Zurich, Switzerland : s.n., 2013.

56. Hoog, Andrew. Forensic Security Analysis of Google Wallet. *nowsecure.* [Online] December 12, 2011. https://www.nowsecure.com/blog/2011/12/12/forensic-security-analysis-of-google-wallet/.

57. android pay. [Online] 2015. https://www.android.com/pay/#.

58. Google Developers-Guides. [Online] 2015. https://developers.google.com/android-pay/integration/gateway-processor-integration.

59. Killian, Joe. *Theory of Cryptography.* Princeton : Springer, 2005.

60. Ohad Bobrov, Avi Bashan. *Certifi_Gate: Front Door Access to Pwing Millions of Android Devices.* s.l. : Check Point Software Technologies, 18072015.

61. Apple Pay. *Wikipedia.* [Online] November 19, 2015. https://en.wikipedia.org/wiki/Apple_Pay.

62. Mahmud, Norshidah M. Mantoro T. Media Ayu Murni. *Critical Socio-Technical Issues Surrounding Mobile Computing.* s.l. : IGI Global(Information Science Reference), 2015.