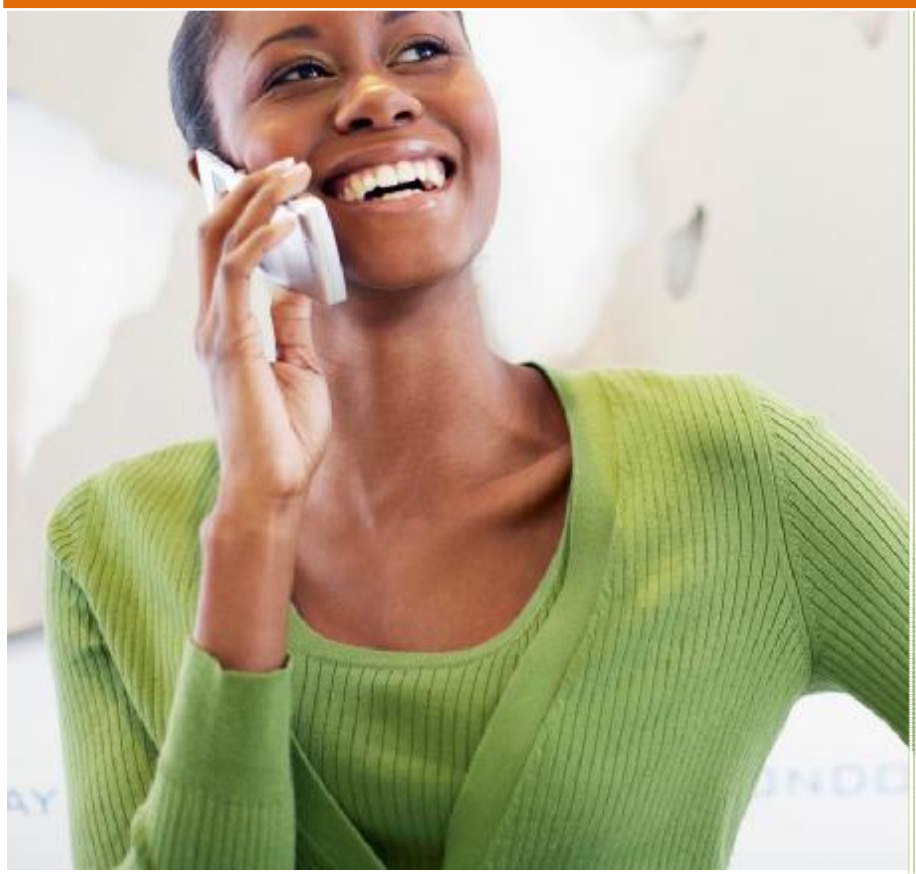
Πανεπιστήμιο Πειραιά
Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων

Μελέτη των Μηχανισμών Ασφάλειας στα Δίκτυα Νέας Γενιάς



Βασίλης Αγγελόπουλος, ΜΕ/0561

Επιβλέπων Καθηγητής, Χρήστος

Πειραιάς, 06/04/2008

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

1. ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγή στα 3G Δίκτυα

Καθ' όλη τη διάρκεια των δεκαετιών η ανάγκη για πανταχού παρούσες επικοινωνίες έχει οδηγήσει και έχει ενθαρρύνει την ανάπτυξη, και την επέκταση, διάφορων τεχνολογιών για να παρέχει στους χρήστες αποτελεσματικά κινητά μέσα επικοινωνίας. Οι διευθυντές, οι υποδιευθυντές και οι επιχειρησιακοί άνθρωποι γενικά πρέπει να έχουν πρόσβαση στις πληροφορίες των εταιριών τους ενώ κινούνται, να συμβουλευθούν τις πληροφορίες σχετικά με το χρηματιστήριο, καθώς επίσης και καλούν τις οικογένειες και τους υπαλλήλους τους. Για το υπόλοιπο των ανθρώπων, οι κινητές επικοινωνίες αντιπροσωπεύουν μια μεγάλη ευκαιρία να διατηρήσουν επαφή ο ένας με τον άλλο με την ανταλλαγή των μηνυμάτων, τη συμμετοχή στις φωνητικές συνομιλίες και τη διαβίβαση δεδομένων σε/από το Διαδίκτυο και όλοι μέσω των χαμηλής ισχύος κινητών τηλεφώνων.

Η πρόταση τρίτης γενεάς (3G) για τις κινητές επικοινωνίες υποστηρίζει ότι παρέχει ένα παγκόσμιο roaming, υψηλά ποσοστά μεταφοράς δεδομένων και προηγμένες υπηρεσίες όπως: υπηρεσίες εμπορίου, global positioning system και μηνύματος πολυμέσων μέσω ήχου και εικόνας. Όλες αυτές οι πιθανές υπηρεσίες, καθώς επίσης και το είδος των πληροφοριών που μεταδίδεται σε όλο το δίκτυο, καθιστούν τις απαιτήσεις σε ζητήματα ασφάλειας ακόμα σημαντικότερα να εξετάσουν απ' ότι ήταν πριν και κάνουν τις απαιτήσεις ασφάλειας ακόμα ισχυρότερες.

Ότι ο κόσμος είναι έτοιμος να αναπτύξει μια τεχνολογία τρίτης γενεάς για τις κινητές τηλεπικοινωνίες ήταν μια γενικευμένη άποψη κατά τη διάρκεια των τελευταίων δύο δεκαετιών. Τυποποιώντας τις οργανώσεις, οι χειριστές δικτύων και οι κατασκευαστές έχουν ενθαρρύνει τις προσπάθειες ανάπτυξης εδώ και πολύ χρόνο, και ο κόσμος βλέπει τα πρώτα αποτελέσματα τώρα. Το πρώτο 3G δίκτυο στον κόσμο έχει συντηρήσει πληθώρα χρηστών στην Ιαπωνία για περισσότερο από δύο έτη, και είναι μια μεγάλη επιτυχία. Τον Οκτώβριο του 2001 η NTT DoCoMo, η αρχαιότερη επιχείρηση επικοινωνιών της Ιαπωνίας, έβαλε την υπηρεσία κινητών επικοινωνιών τρίτης γενιάς σε λειτουργία για την ιαπωνική αγορά. Αυτή η υπηρεσία καλείται

Freedom Of Mobile multimedia Access (FOMA). Τα βασικά πλεονεκτήματα για τους χρήστες περιλαμβάνουν:

- Η δυνατότητα να μιλήσει σε έναν άλλο χρήστη, πρόσωπο με πρόσωπο, από το βιντεόφωνο.
- Εντυπωσιακά υψηλά ποσοστά για τη μετάδοση δεδομένων.
- Ταυτόχρονη επικοινωνία για φωνή και μετάδοση δεδομένων.
- Η ικανότητα να κατεβάσει (download) και να στείλει σε email περιεχόμενο πολυμέσων.
- Συνεδρίαση μέσω video μέχρι και οκτώ συμμετεχόντων(Videoconferencing).
- Ασφαλής αγορές χάρη στα υψηλά επίπεδα εμπιστευτικότητας και επικύρωσης
- Κινητή υπηρεσία Διαδικτύου I-mode

Τον Δεκέμβριο του 2005, 100 3G δίκτυα λειτουργούσαν σε 40 χώρες, σύμφωνα με το Global mobile Suppliers Association. Στην Ασία, την Ευρώπη, τον Καναδά και τις ΗΠΑ, οι επιχειρήσεις τηλεπικοινωνιών χρησιμοποιούν τη τεχνολογία W- CDMA και με την υποστήριξη περίπου 100 κατασκευαστών κινητών τηλεφώνων σχεδιάζει να ενεργοποιήσει νέα 3G κινητά δίκτυα.

Στην Ευρώπη, οι 3G υπηρεσίες εισήχθησαν αρχικός τον Μάρτιο του 2003 στην Αγγλία και την Ιταλία. Το Συμβούλιο της Ευρωπαϊκής Ένωσης πρότεινε ότι οι 3G πάροχοι πρέπει να καλύψουν το 80% των ευρωπαϊκών εθνικών πληθυσμών μέχρι το τέλος του 2005.

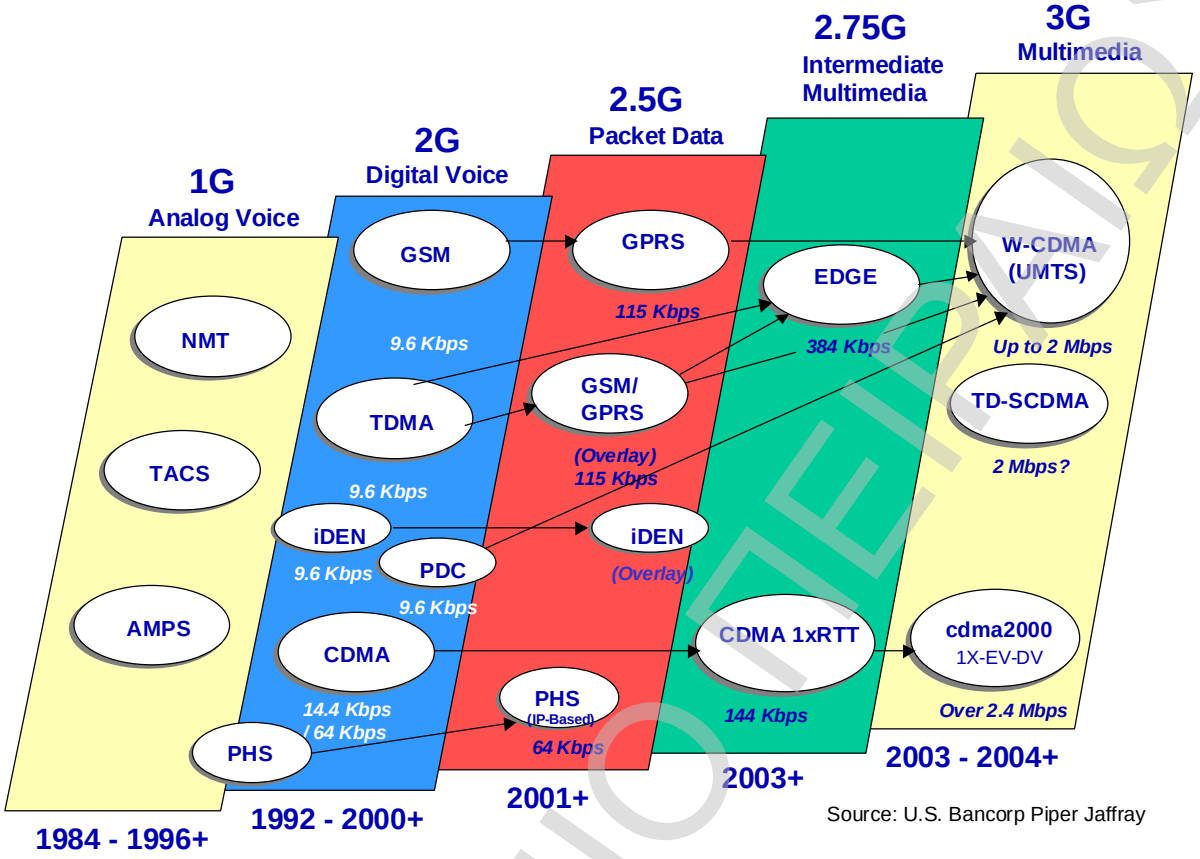
Η εφαρμογή των 3G δικτύων σε μερικές χώρες καθυστέρησε από τις τεράστιες δαπάνες των αμοιβών χορήγησης αδειών φάσματος. Σε πολλές χώρες, τα 3G δίκτυα δεν χρησιμοποιούν τις ίδιες ραδιοσυχνότητες με το 2G, και έτσι οι πάροχοι πρέπει να χτίσουν εξ ολοκλήρου τα νέα δίκτυα και τις νέες συχνότητες εξ ολοκλήρου. Μια εξαίρεση είναι οι Ηνωμένες Πολιτείες όπου οι πάροχοι διεκπεραιώνουν τη 3G υπηρεσία στις ίδιες συχνότητες με τις άλλες υπηρεσίες. Οι αμοιβές αδειών σε μερικές ευρωπαϊκές χώρες ήταν ιδιαίτερα υψηλές, υποστηριγμένες από κυβερνητικές δημοπρασίες ενός περιορισμένου αριθμού αδειών και τις σφραγισμένες δημοπρασίες προσφοράς, και τον αρχικό ενθουσιασμό πέρα από τη δυνατότητα του 3G. Άλλες

καθυστερήσεις οφείλονται στις δαπάνες της αναβάθμισης του εξοπλισμού για τα νέα συστήματα.

Από τον Ιούνιο του 2007 ο διακοσιοστός εκατομμυριοστός 3G συνδρομητής ήταν συνδεμένος. Από τα 3 δισεκατομμύρια κινητές τηλεφωνικές συνδρομές παγκοσμίως αυτό είναι μόνο 6,7%. Στις χώρες όπου το 3G προωθήθηκε πρώτα, Ιαπωνία και Νότια Κορέα, πάνω από τη μισή από όλη τη χρήση είναι για το 3G. Στην Ευρώπη που η κορυφαία χώρα είναι Ιταλία με ένα τρίτο των συνδρομητών της στο 3G. Σε άλλες χώρες περιλαμβανομένων της Αγγλίας, της Αυστρίας και της Σιγκαπούρης το ποσοστό έφτασε μέχρι το 20%.

Μεγάλο ενδιαφέρον για την ανάπτυξη των 3G δικτύων υπάρχει παγκοσμίως και διάφορες επιχειρήσεις έχουν επενδύσει μέρη των χρημάτων σε αυτήν την προσπάθεια. Κατά συνέπεια, αυτή η τεχνολογία θα αλλάξει δραστικά τον τρόπο της διαβίωσης της κοινωνίας στα επόμενα έτη. Όχι μόνο είναι απαραίτητο να επεκταθούν τα δίκτυα, αλλά οι υπηρεσίες που παρέχουν πρέπει να προωθηθούν, να γίνουν πιο αξιόπιστες και ασφαλής προκειμένου να ικανοποιηθούν οι προσδοκίες του πελάτη. Η κάλυψη αυτών των απαιτήσεων δεν είναι ένας εύκολος στόχος δεδομένου ότι διάφορες σύνθετες διαδικασίες διενεργούνται σε όλο το δίκτυο που πρέπει να εξεταστεί προσεκτικά προκειμένου αυτές να εφαρμοστούν με έναν αποδοτικό τρόπο.

Αλλά τι είναι πραγματικά το 3G; Ένας καθορισμός που η DoCoMo δίνει είναι ο ακόλουθος: Τεχνολογία κινητών τηλεφώνων τρίτης γενιάς. Ένα ψηφιακό κινητό τηλεφωνικό σύστημα που τυποποιείται από το ITU-T (International Telecommunication Union Telecommunication Standardization Sector), και είναι επίσης γνωστό ως IMT -2000. Το ποσό μεταφοράς δεδομένων(data rate) είναι 144 kbps για τη γρήγορη κίνηση, 384 kbps για την πιο αργή κίνηση και 2 Mbps όταν το κινητό-τερματικό είναι στάσιμο.



Το σημαντικότερο χαρακτηριστικό γνώρισμα της 3G τεχνολογίας είναι ότι υποστηρίζει μεγαλύτερους αριθμούς πελατών για φωνή και δεδομένα, ειδικά στις αστικές περιοχές, και υψηλότερα ποσοστά μεταφοράς δεδομένων με χαμηλότερο κόστος από το 2G. Με τη χρησιμοποίηση του ραδιοφάσματος στις ζώνες που προσδιορίστηκαν, που παρέχεται από το UTI για τις κινητές υπηρεσίες Third Generation IMT-2000, χορηγηθήκαν άδειες στη συνέχεια στους πάροχους. Το 3G χρησιμοποιεί 6 MHz πλάτος μεταφορέων καναλιών για να παραδώσει τα σημαντικά υψηλότερα ποσά μεταφοράς δεδομένων και την αυξανόμενη ικανότητα έναντι του 2G στα δίκτυα.

Το 5 MHz κανάλι παρέχει βέλτιστη χρήση των ραδιο πόρων για τους πάροχους που τους έχουν χορηγηθεί μεγάλα, διπλανά blocks του φάσματος. Επίσης, βοηθά να μειώθει το κόστος του 3G στα δίκτυα ενώ είναι και σε θέση για εξαιρετικά γρήγορη μετάδοση δεδομένων στους χρήστες. Επιτρέπει επίσης τη μετάδοση 384 kbit/s για τα κινητά συστήματα και 2 Mb/s για τα στάσιμα συστήματα. Οι 3G χρήστες αναμένονται να έχουν μεγαλύτερη ικανότητα και καλύτερη αποδοτικότητα του

φάσματος, η οποία επιτρέπει σε αυτούς για να έχουν πρόσβαση στο παγκόσμιο roaming μεταξύ διαφορετικών 3G δικτύων.

1.2 Εισαγωγή στο UMTS

Το ακρωνύμιο UMTS σημαίνει Universal Mobile Telecommunications System. Το UMTS είναι μια από τις νέες τεχνολογίες κινητής τηλεφωνίας που αναπτύσσονται και είναι γνωστές ως τρίτης-γενιάς, ή 3G. Τα συστήματα τρίτης-γενιάς σχεδιάζονται για να έχουν λειτουργίες όπως τα παραδοσιακά τηλέφωνα ,όπως τις κλήσεις, το φωνητικό ταχυδρομείο, και τη σελιδοποίηση, αλλά και λειτουργίες νέας τεχνολογίας όπως η πρόσβαση Διαδικτύου, το βίντεο και το SMS.

Ένα από τα κύρια οφέλη του UMTS είναι η ταχύτητά του. Τα τρέχοντα ποσοστά μεταφοράς δεδομένων για τις ευρυζωνικές πληροφορίες είναι 2 Mbits το δευτερόλεπτο. Αυτή η ταχύτητα καθιστά πιθανό το είδος του streaming video που μπορεί να υποστηρίξει το download ταινιών και την τηλεοπτική σύσκεψη (video conferencing). Θα μπορούσαμε να πούμε ότι το UMTS καθιστά πιθανό για εμάς να απολαύσουμε όλη την λειτουργία του υπολογιστή μας ενώ περιπλανιόμαστε (roaming). Με το συνδυασμό των ασύρματων και δορυφορικών κυψελοειδών τεχνολογιών, το UMTS εκμεταλλεύεται όλες τις υπάρχουσες επιλογές για να μας οδηγήσει στο 3G .

Το UMTS μπήκε σε λειτουργία σε δίκτυο για πρώτη φορά στην Ιαπωνία το 2001. Η Αυστρία είχε το δικό της δίκτυό δύο έτη αργότερα. Μια ομάδα άλλων ευρωπαϊκών χωρών ακολούθησε τη μόδα του UMTS στα επόμενα δύο έτη, με τη Νότια Αφρική και μερικές άλλες χώρες της Αφρικής σύντομα να ακολουθούν. Οι ΗΠΑ έχουν χρησιμοποιήσει τα δίκτυα UMTS σε διάφορες μεγάλες πόλεις, και ο αριθμός αυξάνεται σταθερά.

Το UMTS είναι βασισμένο στο Global System for Mobile (GSM), το οποίο είναι το «χρυσό» πρότυπο σε Ευρώπη και σε περισσότερες από 120 χώρες παγκοσμίως. Στην πραγματικότητα, το UMTS αναφέρεται μερικές φορές ως 3GSM. Τα δύο συστήματα δεν είναι συμβατά, εντούτοις. Το UMTS δεν είναι συμβατό με το GSM. Μερικά

τηλέφωνα είναι dual, GSM/UMTS, αλλά εκτός αν εκείνο το νέο κινητό τηλέφωνο ή συσκευή στην οποία δεν μπορείτε να περιμένετε να πάρετε τα χέρια σας υποστηρίζει dual, εσείς θα είναι σε θέση μόνο να χρησιμοποιήσει το έναν τρόπο, αυτόν που ήρθε με τη συσκευή.

Οι βασικές ασύρματοι παράμετροι, δικτύων και υπηρεσιών του συστήματος UMTS καθορίστηκαν από το European Telecommunications Standards Institute (ETSI) στις αρχές του 1998. Στο ETSI ανέπτυξαν τα εξαιρετικά επιτυχή πρότυπα GSM δεύτερης γενεάς (Global System for Mobile communications) που χρησιμοποιούνται από πάνω από 650 εκατομμύριο πελάτες παγκοσμίως και αποτελούν περίπου το 70% της ασύρματης αγοράς επικοινωνιών. Ένα σημαντικό χαρακτηριστικό του UMTS είναι ότι το νέο ραδιο δίκτυο πρόσβασης θα συνδεθεί με μια εξέλιξη του κεντρικού δικτύου GSM.

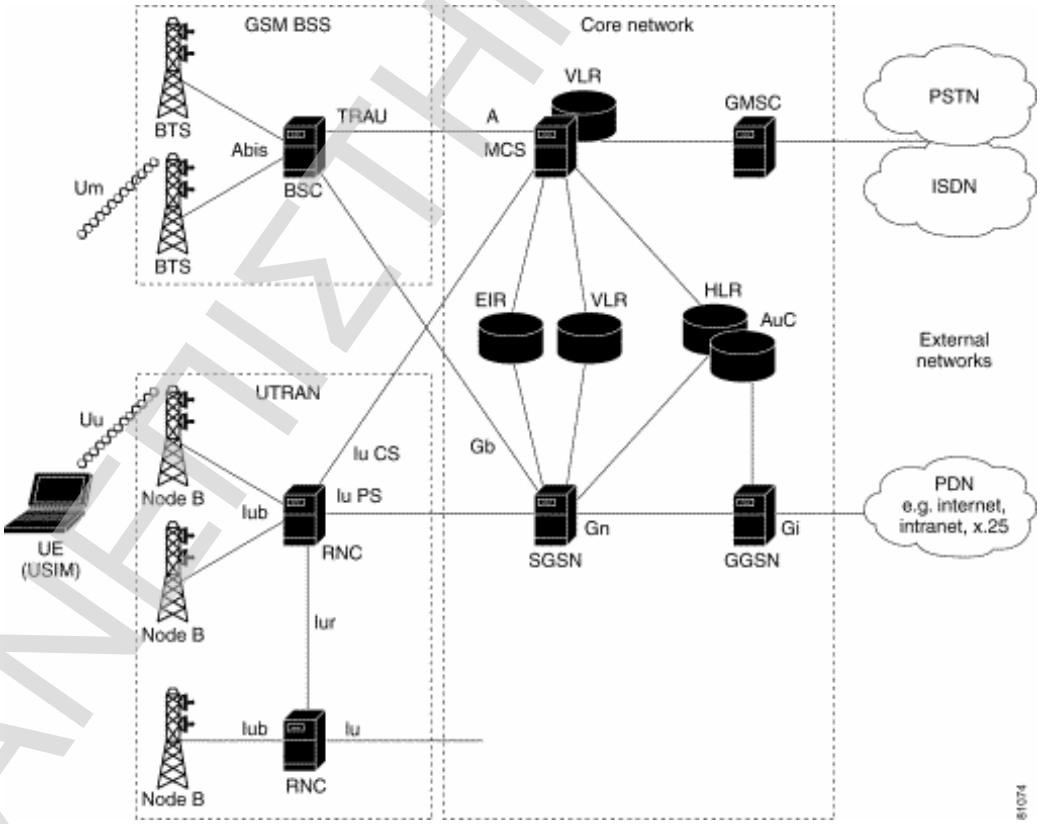
Για να βοηθηθεί και να στηριχτεί στη παγκόσμια επιτυχία του GSM, τοUMTS πρότυπο από το ETSI μεταφέρθηκε το 1998 σε μια παγκόσμια συνεργασία των περιφερειακών οργανισμών προτύπων αποκαλούμενων 3GPP (3rd Generation Partnership Project). Μια χωριστή συνεργασία των οργανισμών προτύπων, γνωστή ως 3GPP, αναπτύσσει ένα άλλο τρίτο κυψελοειδές σύστημα γενιάς κινητών βασισμένο σε διαφορετικά 3G ραδιο πρότυπα διεπαφών αποκαλούμενο CDMA2000 και ένα κεντρικό δίκτυο που εξελίσσεται από τα βορειοαμερικανικά πρότυπα ANSI-41. Μια από τις πτυχές του GSM που έχει παίξει έναν σημαντικό ρόλο στη παγκόσμια πρόοδο του είναι το σύνολό της χαρακτηριστικών γνωρισμάτων ασφάλειας. Η ασφάλεια του UMTS στηρίζεται στην επιτυχία του GSM με την παροχή νέων και ενισχυμένων χαρακτηριστικών γνωρισμάτων ασφάλειας.

Το UMTS προσφέρει τις τηλευπηρεσίες (όπως την ομιλία ή το SMS) και τις υπηρεσίες φορέων(bearer services), οι οποίες παρέχουν την ικανότητα για τη μεταφορά πληροφοριών μεταξύ των σημείων πρόσβασης. Είναι δυνατό να συζητηθούν και να επαναδιαπραγματευθούν τα χαρακτηριστικά μιας υπηρεσίας φορέων στην καθιέρωση συνόδου ή σύνδεσης και κατά τη διάρκεια της τρέχουσας συνόδου ή της σύνδεσης. Και οι connection oriented αλλά και οι connectionless υπηρεσίες προσφέρονται και σε Point-to-Point αλλά και σε Point-to-Multipoint επικοινωνία.

1.3 UMTS Τεχνικές Προδιαγραφές

Το UMTS έχει ένα Virtual Home Environment (VHE). Είναι μια έννοια για την προσωπική φορητότητα του περιβάλλοντος υπηρεσιών στα όρια των δικτύων και μεταξύ των τερματικών. Το Virtual Home Environment σημαίνει ότι οι χρήστες έχουν πάντα τα ίδια εξατομικευμένα χαρακτηριστικά γνωρίσματα, το δικό τους User Interface και τις υπηρεσίες σε οποιοδήποτε δίκτυο ή τερματικό, οπουδήποτε ο χρήστης μπορεί και να βρεθεί. Το UMTS επίσης έχει βελτιώσει την ασφάλεια των δικτύων και τις υπηρεσίες.

Ένα δίκτυο UMTS αποτελείται από τρία αλληλεπιδρώμενα domains. Το κεντρικό δίκτυο (Core Network, CN), το επίγειο ραδιο-δίκτυο πρόσβασης UMTS (UMTS Terrestrial Radio Access Network, UTRAN) και τον εξοπλισμό (UE) των χρηστών. Η κύρια λειτουργία του κεντρικού δικτύου είναι να παρασχεθεί η μετατροπή, η δρομολόγηση και η διέλευση (switching, routing and transit) της κυκλοφορία των χρηστών. Το κεντρικό δίκτυο περιέχει επίσης τις βάσεις δεδομένων και τις διοικητικές λειτουργίες της διαχείρισης δικτύων.



1.3.1 UMTS Τεχνικές Προδιαγραφές (Κεντρικό δίκτυο - Core Network)

Η βασική δικτυακή αρχιτεκτονική για το UMTS (Core Network) είναι βασισμένη στο δίκτυο GSM με GPRS. Όλος ο εξοπλισμός πρέπει να τροποποιηθεί για τη λειτουργία και τις υπηρεσίες του UMTS. Το UTRAN παρέχει τη μέθοδο ασύρματης προσπέλασης των διεπαφών για τον εξοπλισμό των χρηστών(User Equipment). Ο σταθμός βάσεων(Base Station) αναφέρεται και ως κόμβος-Β και ο εξοπλισμός ελέγχου για τους κόμβος-Β καλείται Radio Network Controller (RNC).

Το κεντρικό δίκτυο(Core Network) διαιρείται σε circuit switched και packet switched domains. Μερικές από τις circuit switched οντότητες είναι το Mobile services Switching Centre (MSC), ο κατάλογος θέσης επισκεπτών (Visitor location register, VLR) και το Gateway MSC. Οι packet switched οντότητες εξυπηρετούν το Serving GPRS Support Node (SGSN) και το Gateway GPRS Support Node (GGSN). Μερικές οντότητες των δικτύων, όπως τα EIR, HLR, VLR και AUC μοιράζονται και από τα δύο domains.

Ο τρόπος ασύγχρονης μεταφοράς (Asynchronous Transfer Mode, ATM) καθορίζεται για τη κύρια μετάδοση (core transmission) στο UMTS. Το ATM Adaptation Layer type 2 (AAL2) χειρίζεται τις circuit switched συνδέσεις και το πρωτόκολλο AAL5 (packet connection protocol) την διανομή των δεδομένων.

Η αρχιτεκτονική του κεντρικού δικτύου(Core Network) μπορεί να αλλάξει όταν εισάγονται νέες υπηρεσίες και χαρακτηριστικά γνωρίσματα. Η Number Portability DataBase (NPDB) θα χρησιμοποιηθεί για να επιτρέψει στο χρήστη να αλλάξει το δίκτυο κρατώντας τον παλαιό τηλεφωνικό αριθμό του. Το Gateway Location Register (GLR) μπορεί να χρησιμοποιηθεί για να βελτιστοποιήσει το χειρισμό συνδρομητών μεταξύ των διαδικτυακών ορίων. Το MSC, VLR και SGSN μπορούν να συγχωνευτούν για να γίνουν ένα UMTS MSC.

Οι Mobile services Switching Center (MSC) υπηρεσίες είναι το κύριο συστατικό του CS domain. Είναι η διεπαφή μεταξύ του κυψελοειδούς δικτύου και των εξωτερικών

σταθερών circuit-switched τηλεφωνικών δικτύων όπως το PSTN. Αυτό το συστατικό εκτελεί τη δρομολόγηση των κλήσεων από το εξωτερικό δίκτυο σε έναν μεμονωμένο κινητό σταθμό και όλων των λειτουργιών switching και signaling για τους κινητούς σταθμούς που βρίσκονται σε μια γεωγραφική περιοχή που υποδεικνύεται ως περιοχή MSC. Οι πρόσθετες λειτουργίες περιλαμβάνουν:

- Πραγματοποίηση των διαδικασιών που απαιτούνται για την εγγραφή και την παράδοση θέσης (location registration and handover)
- Συλλογή των στοιχείων για λόγους χρέωσης
- Διαχείριση παραμέτρων κρυπτογράφησης

Τα πρόσθετα MSCs μπορούν να συνυπάρξουν μέσα στο κυψελοειδές δίκτυο εάν η κυκλοφορία απαιτεί περισσότερη ικανότητα ανταλλαγής από τη παρεχόμενη από ένα από αυτά. Η διεπαφή IuCS συνδέει το MSC με το RNC στο UTRAN και μερικές διεπαφές υπάρχουν στο PS domain, το PSTN, το MSC και τα τμήματα εγγραφής στο δίκτυο.

Ο Home Location Register (HLR) είναι η οντότητα που αποθηκεύει τα στοιχεία σχετικά με κάθε συνδρομητή των υπηρεσιών που παρέχονται από το δίκτυο κινητής τηλεφωνίας. Αυτές οι πληροφορίες εισάγονται όταν μπαίνει ο χρήστης στο δίκτυο. Υπάρχουν δύο είδη πληροφοριών σε ένα HLR: μόνιμα και προσωρινά. Το μόνιμο στοιχείο δεν αλλάζει εκτός αν μια παράμετρος συνδρομής πρέπει να τροποποιηθεί. Τα προσωρινά στοιχεία αλλάζουν συνεχώς, ακόμη και από κλήση σε κλήση, και μερικά στοιχεία μπορεί να μην είναι πάντα απαραίτητα. Τα μόνιμα δεδομένα σχετικά για τους σκοπούς αυτής της έκθεσης περιλαμβάνουν το IMSI και ένα κλειδί αυθεντικοποίησης. Ένα δίκτυο κινητής τηλεφωνίας μπορεί να έχει διάφορα HLRs ανάλογα με το μέγεθος της περιοχής κάλυψής του.

Ο κατάλογος θέσης επισκεπτών (Visitor Location Register, VLR) είναι το συστατικό που εφαρμόζεται σχετικά με ένα MSC. Το VLR φυλάσσει τις πληροφορίες σχετικές με κάθε κινητό σταθμό που περιπλανάτε στην περιοχή που συντηρείται από το σχετικό MSC. Κατά συνέπεια, το VLR περιέχει τις πληροφορίες για τους ενεργούς συνδρομητές στο δίκτυό του, ακόμη και από εκείνους στους οποίους αυτό το δίκτυο

είναι το εγχώριο δίκτυό τους (home network). Όταν ο συνδρομητής αλλάζει διαφορετικά δίκτυα, οι πληροφορίες του HLR του, αντιγράφονται στο VLR σε κάθε δίκτυο που επισκέπτεται, και χάνονται όποτε ο συνδρομητής αφήνει εκείνο το δίκτυο. Οι πληροφορίες που αποθηκεύονται από το VLR είναι σχεδόν οι ίδιες με αυτές που αποθηκεύονται από το HLR.

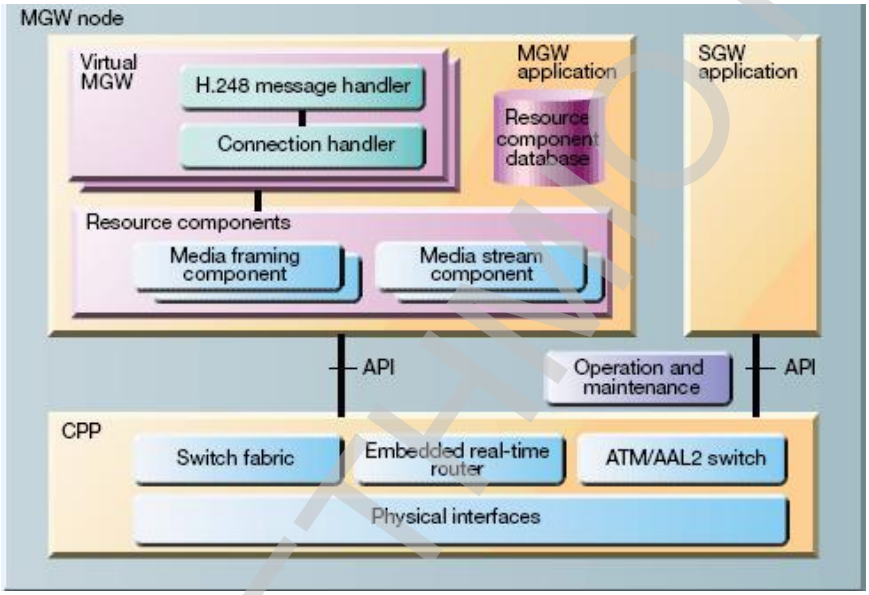
Το κέντρο αυθεντικοποίησης (Authentication Center, AuC) σε φυσικό επίπεδο υπάρχει σε ένα HLR. Αυτό η οντότητα αποθηκεύει, για κάθε συνδρομητή, ένα κλειδί αυθεντικοποίησης K καθώς επίσης και την αντιστοιχία IMSI, τα οποία είναι μόνιμα στοιχεία που εισάγονται στο χρόνο συνδρομής. Το AuC διαδραματίζει έναν κρίσιμο ρόλο στην αρχιτεκτονική ασφάλειας του δικτύου, δεδομένου ότι είναι αρμόδιο της παραγωγής των σημαντικών στοιχείων που χρησιμοποιούνται στις διαδικασίες αυθεντικοποίησης και κρυπτογράφησης.

Το Serving GPRS Support Node (SGSN) είναι αρμόδιο για τη διαχείριση της κινητικότητας και τη διαχείριση των πακέτων IP. Καθοδηγεί την κυκλοφορία των πακέτων δεδομένων των χρηστών από το ραδιο-δίκτυο πρόσβασης (radio access network) στον κατάλληλο Gateway GPRS Support Node, το οποίο παρέχει στη συνέχεια την πρόσβαση στα εξωτερικά δίκτυα δεδομένων. Επιπλέον, παράγει τα αρχεία που χρησιμοποιούνται από άλλες οντότητες για λόγους χρέωσης. Το SGSN βοηθά να ελέγξει την πρόσβαση στους πόρους των δικτύων, και αποτρέπει την αναρμόδια πρόσβαση στο δίκτυο ή συγκεκριμένες υπηρεσίες και εφαρμογές. Η διεπαφή IuPS συνδέει το SGSN, το κύριο συστατικό της περιοχής PS, με το RNC στο UTRAN.

Το Gateway GPRS Support Node (GGSN) είναι η πύλη μεταξύ του κυψελοειδούς δικτύου και των εξωτερικών δικτύων δεδομένων όπως το Διαδίκτυο και τα εταιρικά intranets. Σαν το συνεργάτη του το SGSN, και άλλες οντότητες, το GGSN συλλέγει επίσης τις πληροφορίες χρέωσης, που διαβιβάζονται στη Charging Gateway Function (CGF), για λόγους χρέωσης.

Το Equipment Identity Register (EIR) είναι μια βάση δεδομένων που κρατά έναν κατάλογο κινητών τηλεφώνων (που προσδιορίζονται από IMEI τους), τα οποία πρόκειται να απαγορευθούν από το δίκτυο ή να ελεγχθούν.

Η UMTS Media Gateway είναι αρμόδια για την αλλαγή του φορέα. Το MGW μπορεί επίσης να χρησιμοποιηθεί για να μετατρέψει την κυκλοφορία φορέων μεταξύ δύο διαφορετικών formats. Παραδείγματος χάριν, του PCM circuit voice σε VoP. Το MGW περιέχει transcoders και άλλον ακουστικό εξοπλισμό. Τα Media gateways έχουν εισαχθεί για να γεφυρώσουν το χάσμα μεταξύ των διαφορετικών τεχνολογιών μετάδοσης δεδομένων και για να προσθέσουν την υπηρεσία στις συνδέσεις τελικών χρηστών. Η ομαλή βαθμιαία μετανάστευση προς τη νέα δικτυακή αρχιτεκτονική επιτυγχάνεται με το διαχωρισμό των κινητών υπηρεσιών του switching center (MSC) και τον serving GPRS support node (SGSN) σε media gateway και κεντρικούς υπολογιστές.



Λειτουργική αρχιτεκτονική του ***media gateway***

1.3.2 UMTS Τεχνικές Προδιαγραφές (UTRAN)

Η τεχνολογία Wide band CDMA επιλέχτηκε για τη διεπαφή αέρα του UTRAN. Το UMTS WCDMA είναι ένα σύστημα Direct Sequence CDMA όπου τα δεδομένα των χρηστών πολλαπλασιάζονται με τα σχεδόν-τυχαία κομμάτια που προέρχονται από τους WCDMA Spreading codes. Στο UMTS, εκτός από το channelisation, οι κώδικες χρησιμοποιούνται για το συγχρονισμό και το ανακάτωμα(scrambling). Το WCDMA έχει δύο βασικούς τρόπους λειτουργίας: Frequency Division Duplex (FDD) και Time

Division Duplex (TDD). Τα κύρια συστατικά του UTRAN είναι δύο. Κόμβος B(Node B) και ασύρματος ελεγκτής δικτύων (Radio Network Controller).

Ο κόμβος B (Node B) είναι ο σταθμός πομποδεκτών βάσεων (base transceiver station) του UTRAN που εξυπηρετεί ένα ή περισσότερα κελιά (cells). Μερικές από τις λειτουργίες του περιλαμβάνουν: ανίχνευση λάθους στα κανάλια και ένδειξη του στα υψηλότερα στρώματα, διαμόρφωση/αποδιαμόρφωση (modulation/demodulation) των φυσικών καναλιών, ραδιο-μετρήσεις και ειδοποίηση για αυτήν στα μεγαλύτερα στρώματα και στάθμιση δύναμης. Μερικοί προμηθευτές προσφέρουν τους σταθμούς βάσεων που υποστηρίζουν και τα πρότυπα UMTS και CDMA2000 μέσω της χρήσης των field-replaceable modules και ενός υψηλού ποσοστού σε συμβατά υλικά και λογισμικό. Η διεπαφή μεταξύ UE και του κόμβου B είναι στην πραγματικότητα μια WCDMA-based UTRA διεπαφή.

Node B, από Lucent Technologies

Ο ραδιο-ελεγκτής δικτύων (Radio Network Controller ,RNC) διαχειρίζεται τους ασύρματους πόρους από κάθε έναν από τους κόμβους B που είναι συνδεδεμένοι με αυτό. Το RNC συνδέεται με το core network's CS domain μέσω της διεπαφής IuCS, και με το PS domain μέσω της διεπαφής IuPS. Όχι μόνο το RNC διαχειρίζεται τους ασύρματους πόρους του εξοπλισμού χρηστών, αλλά είναι μέρος της πορείας σε/από το κεντρικό δίκτυο για τις υπηρεσίες που χρησιμοποιούνται από τον εξοπλισμό χρηστών. Μερικές άλλες δουλειές που εκτελούνται από το RNC περιλαμβάνουν: επεξεργασία της κυκλοφορίας φωνής και δεδομένων, handoff μεταξύ των κελιών και της οργάνωσης και της λήξης των κλήσεων.

Radio Network Controller από τη NEC

Οι κυρίες λειτουργίες του RNC είναι η διαχείριση των ραδιο-καναλιών και των επίγειων καναλιών (προς το MGW και το SGSN). Η λειτουργία της διαχείρισης πόρων (Resource Management) περιλαμβάνει τα εξής:

- Outer Loop Power Control (δείτε επίσης τα loop power control και inner loop power control)
- Load control
- Admission Control
- Packet scheduling
- Handover control
- Macrodiversity combining (δείτε επίσης το macrodiversity)
- Λειτουργίες ασφάλειας
- Διαχείριση κινητικότητας (Mobility Management)

Οι λογικές συνδέσεις μεταξύ των δικτυακών στοιχείων είναι γνωστές ως διεπαφές. Η διεπαφή μεταξύ του RNC και του Circuit Switched Core Network (CS-CN) καλείται Iu-CS και μεταξύ του RNC και του Packet Switched Core Network καλείται IU- Ps. Αλλες διεπαφές περιλαμβάνουν το Iub (μεταξύ του RNC και του κόμβου B) και το Iur (μεταξύ RNCs μέσα στο ίδιο δίκτυο). Οι διεπαφές IU μεταφέρνουν την κυκλοφορία δεδομένων των χρηστών (όπως η φωνή ή τα δεδομένα) καθώς επίσης και ελέγχουν τις πληροφορίες και η διεπαφή Iur απαιτείται κυρίως για τα soft handovers.

Για να συνοψίσουμε, τα ακόλουθα είναι οι νέες διεπαφές UMTS σε σύγκριση με τα δίκτυα GSM/GPRS:

- Iu-CS

Αυτό είναι μια circuit-switched σύνδεση για τη μεταφορά φωνής και δεδομένων μεταξύ του UTRAN και του κεντρικού δικτύου(core network). Αυτό είναι η ισοδύναμη διεπαφή στο δίκτυο GSM/GPRS με την A-διεπαφή(A-interface).

- Iu-PS

Packet-switched σύνδεση για τη μεταφορά δεδομένων και τη σηματοδότηση μεταξύ UTRAN και του δικτύου GPRS (core data GPRS network). Ισοδύναμη διεπαφή στα δίκτυα GSM/GPRS είναι η διεπαφή Gb.

- Lur

Ο αρχικός σκοπός του lur είναι να υποστηριχθεί η κινητικότητα του MSC (inter-MSC mobility). Όταν ένας συνδρομητής κινητής τηλεφωνίας κινείται μεταξύ των περιοχών που εξυπηρετούνται από διαφορετικά RNCs, τα δεδομένα του συνδρομητή μεταφέρονται τώρα στο νέο RNC μέσω του lur. Το αρχικό RNC είναι γνωστό ως Serving RNC και το νέο RNC είναι γνωστό ως Drift RNC. Καμία ισοδύναμη διεπαφή δεν υπάρχει στα δίκτυα GSM/GPRS.

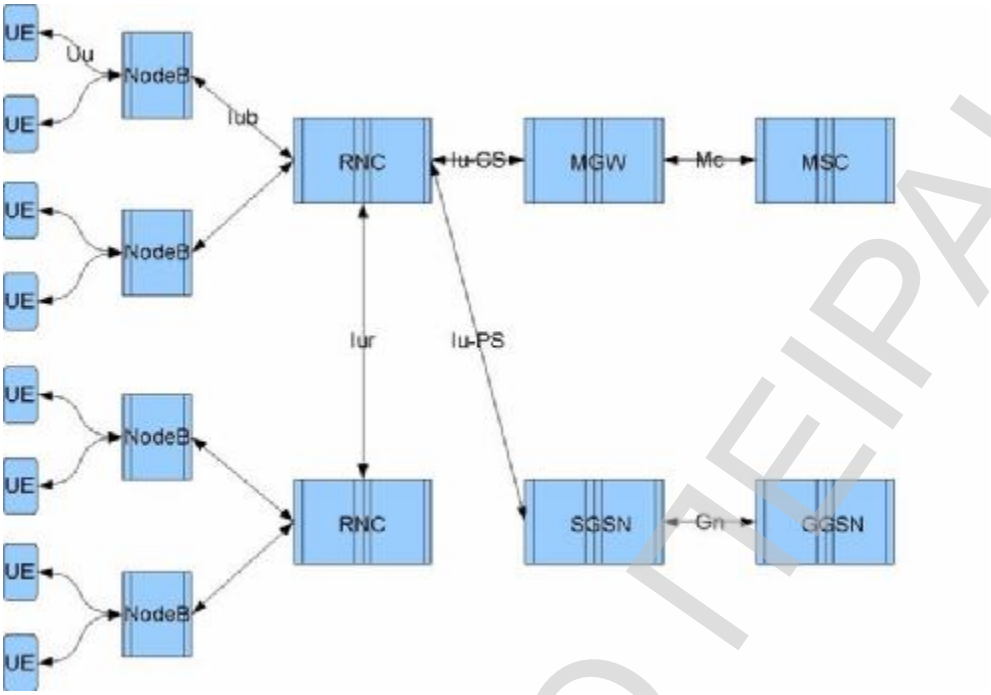
- Lub

Η διεπαφή μεταξύ RNC και των πολλών κόμβων-Β για να ελέγξει τους κόμβους-Β. Η ισοδύναμη διεπαφή στα δίκτυα GSM/GPRS είναι η διεπαφή Abis.

- Uu

Η διεπαφή μεταξύ του εξοπλισμού χρηστών και του κόμβου-Β. Δηλαδή είναι η ασύρματη διεπαφή του UMTS. Η ισοδύναμη διεπαφή στα δίκτυα GSM/GPRS είναι η διεπαφή Um.

Όλες οι διεπαφές στο UTRAN εφαρμόζονται χρησιμοποιώντας το ATM, εκτός από τη διεπαφή Uu που χρησιμοποιεί την τεχνολογία WCDMA. Σε φυσικό επίπεδο, αυτές οι διεπαφές μπορούν να μεταφερθούν σε SDH με την οπτική ίνα, E1 (μερικές φορές καλούμενος PDH) με τα καλωδία ή με μικροκυμάτα. Πολλά Εί μπορεί να συσσωρευθούν για να διαμορφώσουν μια ομάδα IMA. Δεδομένου ότι οι διεπαφές είναι λογικές, πολλές διεπαφές μπορούν να πολλαπλασιαστούν επάνω στην ίδια γραμμή μετάδοσης. Η πραγματική εφαρμογή εξαρτάται από την τοπολογία δικτύων (chain, distant star και loop configurations).



RNC διεπαφές

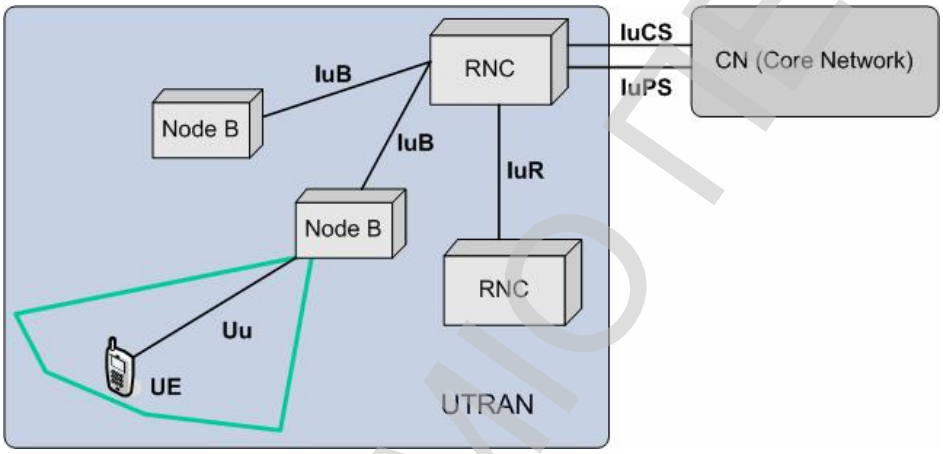
Τα Iub, IU και Iur πρωτόκολλα φέρνουν και τα δεδομένα και τη σηματοδότηση των χρηστών (user data and signalling).

- Το πρωτόκολλο που είναι αρμόδιο για τον έλεγχο του κόμβου Β από το RNC καλείται NBAP (Node-B Application Part). Μερικές φορές το NBAP υποδιαιρείται σε κοινό και αφιερωμένο NBAP (C-NBAP and D-NBAP), όπου το κοινό NBAP ελέγχει τη γενική λειτουργία των κόμβων Β και το αφιερωμένο NBAP ελέγχει τα χωριστά κελλιά ή τους τομείς του κόμβου Β. Το NBAP μεταφέρετε σε Iub.

- Το Control plane πρωτόκολλο για το στρώμα μεταφορών καλείται ALCAP (πρωτόκολλο εφαρμογής ελέγχου συνδέσεων πρόσβασης- Access Link Control Application Protocol). Η βασική λειτουργία του ALCAP είναι να πολλαπλασιάζει τους διαφορετικούς χρήστες επάνω σε ένα AAL2 transmission path χρησιμοποιώντας τα Channel IDs (CIDs). Το ALCAP μεταφέρεται σε Iub.

- Το signalling πρωτόκολλο που είναι αρμόδιο για την επικοινωνία μεταξύ RNC και του κεντρικού δικτύου καλείται RANAP (Radio Access Network Application Part), και μεταφέρεται στη διεπαφή IU.

- Το signalling πρωτόκολλο που αρμόδιο για τις επικοινωνίες μεταξύ των RNCs καλείται RNSAP (Radio Network Subsystem Application Part) και μεταφέρεται στη διεπαφή Iur.



1.3.3 UMTS Τεχνικές Προδιαγραφές (Εξοπλισμός Χρηστών - User Equipment)

Ο εξοπλισμός χρηστών (user equipment) είναι η φυσική συσκευή που χρησιμοποιείται από τους χρήστες. Αποτελείται από έναν κινητό εξοπλισμό (Mobile Equipment -ME) και το UMTS Subscriber Identity Module (USIM). Το USIM είναι μια εφαρμογή που αποθηκεύεται σε μια μετακινούμενη IC κάρτα ολοκληρωμένου κυκλώματος που επικοινωνεί με το ME για να παρέχει την πρόσβαση στις 3G υπηρεσίες.

Το Universal Subscriber Identity Module είναι μια εφαρμογή για την κινητή τηλεφωνία UMTS που τρέχει σε μια έξυπνη κάρτα UICC που εισάγετε σε ένα 3G κινητό τηλέφωνο. Υπάρχει μια κοινή παρερμηνεία ότι η UICC κάρτα είναι το USIM, αλλά το USIM είναι μόνο μια λογική οντότητα στη φυσική κάρτα. Αποθηκεύει τις

πληροφορίες των συνδρομητών-χρηστών, πληροφορίες αυθεντικοποίησης και παρέχει χώρο αποθήκευσης για τα μηνύματα κειμένων και τις επαφές τηλεφωνικών καταλόγων. Ο τηλεφωνικός κατάλογος σε ένα UICC έχει ενισχυθεί πολύ.

Για λόγους αυθεντικοποίησης, το USIM αποθηκεύει ένα μακροπρόθεσμο μυστικό κλειδί (preshared secret key) K, το οποίο μοιράζεται με το κέντρο αυθεντικοποίησης (Authentication Center, AuC) στο δίκτυο. Το USIM ελέγχει επίσης έναν αριθμό ακολουθίας που πρέπει να είναι μέσα σε μια σειρά χρησιμοποιώντας έναν μηχανισμό παραθύρων για να αποφύγει τις επιθέσεις επανάληψης, και είναι υπεύθυνο για την παραγωγή των κλειδιών συνόδου CK και IK που χρησιμοποιείται στους αλγορίθμους εμπιστευτικότητας και ακεραιότητας KASUMI(block cipher) στο UMTS.

Τα πρότυπα UMTS δεν περιορίζουν τη λειτουργία του εξοπλισμού χρηστών από καμιά άποψη. Τα τερματικά λειτουργούν ως μια αντίθετη ασύρματη διεπαφή για τους κόμβος-B(Node-B) και έχουν πολλούς διαφορετικούς τύπους ταυτοτήτων. Οι περισσότεροι από αυτούς τους τύπους ταυτότητας UMTS λαμβάνονται άμεσα από τις προδιαγραφές GSM.

- International Mobile Subscriber Identity (IMSI)
- Temporary Mobile Subscriber Identity (TMSI)
- Packet Temporary Mobile Subscriber Identity (P-TMSI)
- Temporary Logical Link Identity (TLLI)
- Mobile station ISDN (MSISDN)
- International Mobile Station Equipment Identity (IMEI)
- International Mobile Station Equipment Identity and Software Number (IMEISV)

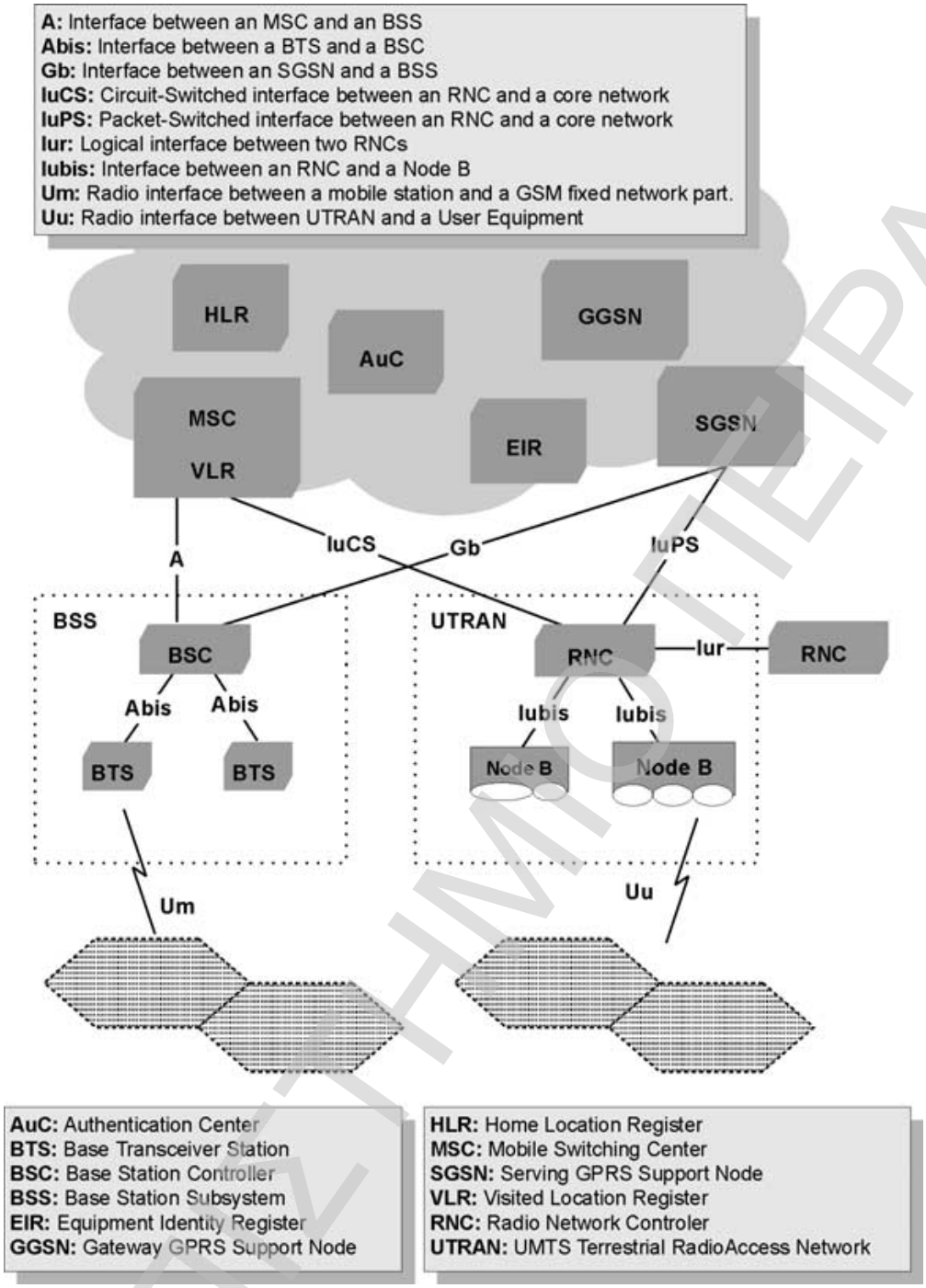
Ο κινητός σταθμός UMTS μπορεί να λειτουργήσει σε έναν από τους τρεις τρόπους λειτουργίας:

- PS (packet switched)/CS (circuit switched) τύπος λειτουργίας: Το MS (mobile station) είναι συνδεμένο και με το PS και το CS domain, και το MS είναι ικανό ταυτόχρονα να λειτουργεί υπηρεσίες PS και CS.

- PS τύπος λειτουργίας: Το MS είναι συνδεμένο με το PS domain μόνο και μπορεί να λειτουργεί μόνο PS υπηρεσίες. Εντούτοις, αυτό δεν αποτρέπει σε CS υπηρεσίες να προσφέρονται από το PS domain.
- CS τύπος λειτουργίας: Το MS είναι συνδεμένο με το CS domain μόνο και μπορεί να λειτουργεί μόνο CS υπηρεσίες.

Η κάρτα ολοκληρωμένου κυκλώματος UMTS έχει τα ίδια φυσικά χαρακτηριστικά με την κάρτα GSM SIM. Έχει διάφορες λειτουργίες:

- Υποστήριξη μιας User Service Identity Module (USIM) εφαρμογής (προαιρετικά και περισσότερες από μια)
- Υποστήριξη ενός ή περισσοτέρων παραμέτρων χρήστη στο USIM
- Αναπροσαρμογή σε συγκεκριμένες πληροφορίες στην USIM όταν λειτουργεί
- Λειτουργίες ασφάλειας
- Αυθεντικοποίηση χρηστών
- Προαιρετικός συνυπολογισμός των μεθόδων πληρωμής
- Προαιρετικό ασφαλές download της νέας εφαρμογής



1.4 Εισαγωγή στην Ασφάλεια στα Δίκτυα Κινητής Τηλεφωνίας

Τα συστήματα κινητών τηλεφώνων πρώτης γενεάς (1G) δεν παρείχαν ουσιαστικά κανένα χαρακτηριστικό γνώρισμα ασφάλειας. Το 2ης γενιάς κινητό σύστημα GSM (2G) σχεδιάστηκε έτσι ώστε παρέχει την ασφάλεια παρόμοια με αυτήν που υπάρχει

στα σταθερά τηλέφωνα, και για να προστατεύσει από την κλωνοποίηση των κινητών ταυτοτήτων (cloning of mobile identities). Το GSM επιτρέπει στο χειριστή δικτύων να ελέγξει την ταυτότητα ενός χρήστη έτσι ώστε είναι ουσιαστικά αδύνατο για κάποιο να μεταμφιεστεί ως γνήσιο χρήστη. Η κρυπτογράφηση των δεδομένων των χρηστών και των πληροφοριών πέρα από τη ασύρματη διεπαφή προστατεύει από το να κρυφακούσει κάποιος(eavesdropping). Στους χρήστες ορίζονται οι προσωρινές ταυτότητες. Αυτά τα χαρακτηριστικά γνωρίσματα αναφέρονται ως επικύρωση, εμπιστευτικότητα και ανωνυμία (authentication, confidentiality and anonymity). Το νέο χαρακτηριστικό γνώρισμα της ασφάλειας GSM είναι η χρήση του Subscriber Identity Module (SIM), το οποίο περιέχει όλο τον προσδιορισμό και τα σχετικά με την ασφάλεια των δεδομένων που ο συνδρομητής χρειάζεται για να κάνει ή να λάβει μια κλήση.

Η ασφάλεια στο UMTS στηρίζεται στην επιτυχία του GSM με τη διατήρηση (και ως ένα ορισμένο βαθμό τη βελτίωση) των σημαντικών και γερών χαρακτηριστικών γνωρισμάτων ασφάλειάς της. Αν και η ασφάλεια του GSM είναι πολύ επιτυχής, ένας στόχος του σχεδίου ασφάλειας UMTS ήταν να εξεταστούν οι πραγματικές και αντιληπτές αδυναμίες του. Μερικές από αυτές τις αδυναμίες είναι οι ακόλουθες:

- ενεργές επιθέσεις που χρησιμοποιούν έναν “ψεύτικο σταθμό βάσεων” (false base station).
- κλειδιά κρυπτογράφησης και δεδομένα αυθεντικοποίησης μεταδίδονται σαν απλό κείμενο μεταξύ και μέσα στα δίκτυα (cipher keys and authentication data are transmitted in clear between and within networks).
- η κρυπτογράφηση δεν επεκτείνεται αρκετά μακριά προς το κεντρικό δίκτυο και τα δεδομένα μεταδίδονται χωρίς κρυπτογράφηση στις συνδέσεις μικροκυμάτων
- δεν παρέχεται ακεραιότητα των δεδομένων.
- η επικύρωση χρηστών σε μια προηγουμένως κλεμμένη σύνοδο εξαρτάται από τη χρήση της κρυπτογράφησης (user authentication on a previously generated cipher key and channel hijack depends on the use of encryption).
- η απάτη και η νομική παρεμπόδιση δεν εξετάστηκαν στη φάση σχεδίου αλλά ήρθαν μόνο ως ύστερες σκέψεις.

- τα 2G συστήματα δεν έχουν την ευελιξία να αναβαθμίσουν και να βελτιώσουν τη λειτουργία ασφάλειας κατά τη διάρκεια του χρόνου.

Εκτός από την αφαίρεση των ανωτέρω παρατηρηθέντων ανεπαρκειών, στο 3G η ασφάλεια προσφέρει τα νέα χαρακτηριστικά γνωρίσματα και υπηρεσίες ασφάλειας. Πρέπει να σημειωθεί ότι ο κύριος στόχος της 3G αρχιτεκτονικής ασφάλειας δεν είναι να παρασχεθεί ένα απολύτως ασφαλές σύστημα, αλλά να χτίσει ένα σύστημα που είναι εύκαμπτο για να προσαρμοστεί στις νέες προκλήσεις.

1.5 Πιθανές Επιθέσεις στα Δίκτυα UMTS

Σε αυτό το τμήμα θα δώσουμε μια σύντομη περιγραφή των επιθέσεων ή των απειλών που εκμεταλλεύονται μια αδυναμία του συστήματος.

- Να κρυφακούσει (Eavesdropping): Ο εισβολέας είναι σε θέση να ακούσει τη σηματοδότηση που συνδέεται άλλους χρήστες ή τις συνδέσεις των δεδομένων τους.
- Πλαστή προσωποποίηση ενός χρήστη (Impersonation of a user): Επιτρέπει στον εισβολέα να αλληλεπιδράσει με το δίκτυο ως ο πραγματικός χρήστης.
- Πλαστή προσωποποίηση του δικτύου (Impersonation of the network): Επιτρέπει στον εισβολέα για να αλληλεπιδράσει με το χρήστη σαν να λαμβάνει τα σήματα από ένα γνήσιο δίκτυο.
- Man-in-the-middle attack: Μια δυνατότητα του εισβολέα να τεθεί μεταξύ δύο επικοινωνούντων συμβαλλόμενων μερών, ενός χρήστη και του δικτύου, επιτρέποντας του διάφορες ενέργειες συμπεριλαμβανομένου να κρυφακούσει, να τροποποιήσει, να διαγραφεί, να ξαναπαραγγείλει, επανάληψη και διάδοση υποκριτικών στοιχείων σηματοδότησης και χρηστών (spoof signaling).
- Compromising authentication vectors in the network: Ο εισβολέας παίρνει τον έλεγχο ενός συμβιβασμένου πίνακα αυθεντικοποίησης (authentication vector) με το συμβιβασμό των κόμβων ή των συνδέσεων δικτύων.

1.6 Μέτρα για την Προστασία Επίθεσης στα Δίκτυα UMTS

Α. Άρνηση της υπηρεσίας (Denial of service)

1) User de-registration request spoofing: Η προστασία ακεραιότητας (integrity) των μηνυμάτων (signaling messages) είναι υποχρεωτική. Το δίκτυο ελέγχει το αίτημα διαγραφής για την ακεραιότητα και την επανάληψη (integrity and replay).

2) Location update request spoofing: Το αίτημα αναπροσαρμογών θέσης προστατεύεται πάντα από την επανάληψη και την τροποποίηση (replay and modification).

3) Camping on a false BS/MS: Η προστασία ακεραιότητας των μηνυμάτων (signaling messages) προστατεύει από την άρνηση της υπηρεσίας μέχρι ενός ορισμένου βαθμού, δεδομένου ότι ο εισβολέας δεν μπορεί να τροποποιήσει τα μηνύματα. Εντούτοις, το σύστημα δεν αποτρέπει τον εισβολέα από την αναμετάδοση των μηνυμάτων μεταξύ του δικτύου και του χρήστη στόχου ή την αγνόηση μερικών από αυτά.

Β. Σύλληψη ταυτότητας (Identity catching)

1) Passive identity catching: Η χρήση των προσωρινών ταυτοτήτων εμποδίζει την παθητική σύλληψη ταυτότητας δεδομένου ότι ο εισβολέας πρέπει να περιμένει μια νέα εγγραφή ή έναν κακό συνδυασμό στην βάση δεδομένων του δικτύου (serving network) προκειμένου να συλληφθεί η μόνιμη ταυτότητα του χρήστη σε απλό κείμενο (plain text).

2) Active identity catching: Το 3G δεν παρέχει την προστασία ενάντια σε αυτόν τον τύπο επίθεσης. Εντούτοις, η ταυτότητα χρηστών δεν είναι ένα χαρακτηριστικό γνώρισμα ασφάλειας.

Γ. Πλαστογράφηση του δικτύου (Impersonation of the network)

1) Με την καταστολή της κρυπτογράφησης μεταξύ του χρήστη στόχου και του εισβολέα (By suppressing encryption between the target user and the intruder): Η επικύρωση στοιχείων και η προστασία επανάληψης μιας υποχρεωτικής κρυπτογραφημένης εντολής (cipher mode command) επιτρέπουν στο κινητό να ελέγξει ότι η ασφάλεια δεν έχει κατασταλεί. Επιπλέον, η διαφάνεια και η διαμόρφωση (visibility and configurability) των χαρακτηριστικών γνωρισμάτων ασφάλειας αποτρέπουν σε μια τέτοια επίθεση να περάσει απαρατήρητη.

2) Με την καταστολή της κρυπτογράφησης μεταξύ του χρήστη στόχου και του δικτύου (by suppressing encryption between the target user and the network): Κατά τη διάρκεια της αρχικής σύνδεσης RRC ο κινητός σταθμός (MS) στέλνει τις δυνατότητες ασφάλειάς του στο SRNC. Αυτές οι δυνατότητες ασφάλειας στέλνονται χωρίς κρυπτογράφηση και μπορούν να τροποποιηθούν (man-in-the-middle). Αλλά, σε ένα μεταγενέστερο στάδιο, το SRNC περιλαμβάνει τις δυνατότητες ασφάλειας των κινητών σταθμών σε μια υποχρεωτικά ασφαλή εντολή (security mode command). Αυτές οι πληροφορίες ενημερώνουν το κινητό σταθμό ότι οι δυνατότητες ασφάλειας είναι άθικτες. Ο κινητός σταθμός λέει στο δίκτυο (serving network) για τις συνεχείς δυνατότητες ασφάλειας σε ένα πλήρες ασφαλές μήνυμα, αφήνοντας τον εισβολέα να έχει πρόβλημα.

3) Με τον αναγκασμό της χρήσης ενός κρυπτογραφημένου κλειδιού (by forcing the use of a compromised cipher key): Η παρουσία ενός αριθμού ακολουθίας στην πρόκληση βοηθά τη προστασία ενάντια στην αναγκασμένη επαναχρησιμοποίηση ενός κρυπτογραφημένου πίνακα αυθεντικοποίησης (authentication vector).

Δ. Πλαστογράφηση χρήστη (Impersonation of the user)

1) Με χρήση κρυπτογραφημένου πίνακα αυθεντικοποίησης (use of a compromised authentication vector)

2) Με την χρήση μιας υποκλεμμένης απάντησης αυθεντικοποίησης (use of an eavesdropped authentication response): Η παρουσία ενός αριθμού ακολουθίας στην πρόκληση προστατεύει από την πολλαπλή χρήση ενός διανύσματος αυθεντικοποίησης (authentication vector).

3) Η πειρατεία των εξερχόμενων κλήσεων στα δίκτυα με την κρυπτογράφηση ενεργοποιημένη/ απενενεργοποιημέμη (Hijacking outgoing calls in networks with encryption disabled/enabled): Ο εισβολέας δεν μπορεί να κλείσει την κρυπτογράφηση. Εντούτοις, η προστασία ακεραιότητας των μηνυμάτων σε κάθε νέα σύνδεση RRC μεταξύ των κινητών σταθμών και του VLR/SGSN είναι υποχρεωτική κάτι που επιτρέπει στο δίκτυο να ελέγξει ότι το αίτημα είναι νόμιμο

4) Πειρατεία των εισερχόμενων κλήσεων στα δίκτυα με απενεργοποιημένη την κρυπτογράφηση (Hijacking incoming calls in networks with encryption disabled): Οι συνδέσεις δέχονται ότι το μήνυμα είναι προστατευμένο στην ακεραιότητα κάτι που επιτρέπει στο δίκτυο να ελέγξει τη νομιμότητά του. Αυτό σημαίνει ότι ο εισβολέας δεν μπορεί να δεχτεί μια σύνδεση εξ ονόματος του χρήστη στόχου. Μετά από την αρχική καθιέρωση σύνδεσης, τα περιοδικά προστατευμένα για ακεραιότητα μηνύματα ανταλλάσσονται κατά τη διάρκεια της σύνδεσης κάτι που προστατεύει από την πειρατεία των μη-κρυπτογραφημένων συνδέσεων

1.7 Επισκόπηση της Αρχιτεκτονικής Ασφαλείας των UMTS Συστημάτων

Η 3G αρχιτεκτονική ασφαλείας καθορίζει πέντε διακριτές περιοχές ασφαλείας, με σκοπό να αναφέρουν συγκεκριμένες απειλές και να εγκαθιδρύσουν τις απαιτούμενες υπηρεσίες ασφαλείας:

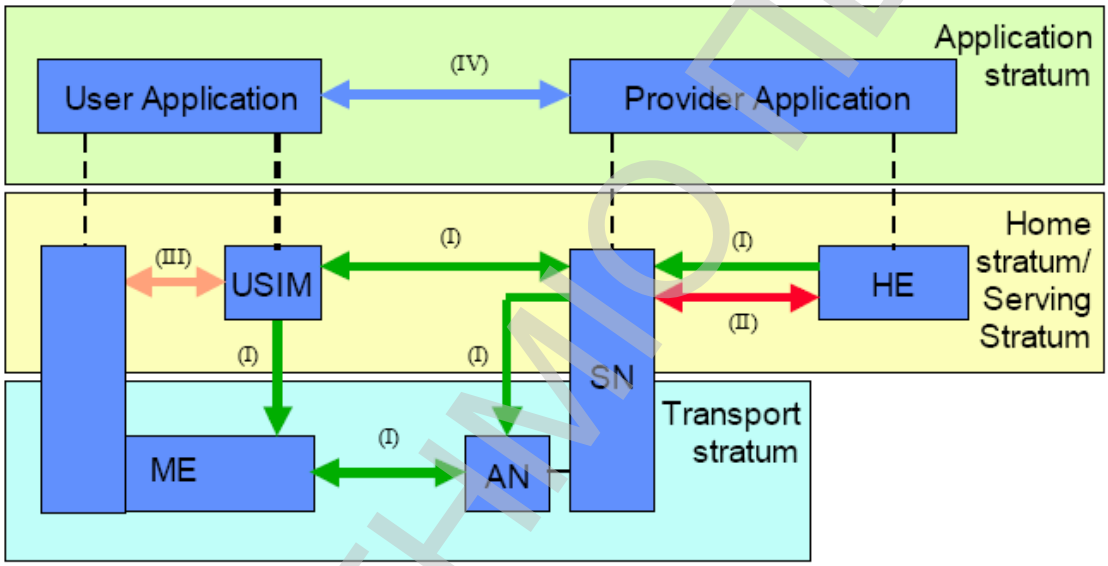
1) Network access security: παρέχει εμπιστευτικότητα της ταυτότητας των χρηστών και των δεδομένων του χρήστη και του συστήματος, προστασία ακεραιότητας των κρίσιμων δεδομένων, επικύρωση του χρήστη και του δικτύου, και προσδιορισμός του κινητού εξοπλισμού.

2) Network domain security: επιτρέπει στους διαφορετικούς κόμβους στο domain του πάροχου να ανταλλάξουν ασφαλώς τα δεδομένα σήματος και προστατεύει από τις επιθέσεις στο δίκτυο γραμμών καλωδίων.

3) User domain security: εξασφαλίζει μόνο εξουσιοδοτημένη πρόσβαση στο Universal Subscriber Identity Module (USIM).

4) Application domain security: επιτρέπει στις εφαρμογές των domains των χρηστών και του πάροχου να ανταλλάξουν ασφαλώς τα μηνύματα.

5) Visibility and configurability of security: ενημερώνει το χρήστη εάν ένα χαρακτηριστικό γνώρισμα ασφάλειας είναι σε λειτουργία και εάν εξαρτηθεί η χρήση και η παροχή υπηρεσιών από το χαρακτηριστικό γνώρισμα ασφάλειας.



Το UMTS παρέχει ενισχυμένη κρυπτογράφηση που εξασφαλίζει ότι τα μηνύματα δεν είναι διαθέσιμα στους αναρμόδιους χρήστες. Με το UMTS, η κρυπτογράφηση ολοκληρώνεται στο radio network controller (RNC) παρά το σταθμό βάσεων (base station), όπως συμβαίνει με το GSM. Η βελτιωμένη εμπιστευτικότητα έχει έρθει περίπου με τη χρησιμοποίηση των πιο μεγάλων σε μήκος κλειδιών κρυπτογράφησης, τα οποία (μαζί με άλλες λειτουργίες ασφάλειας UMTS) είναι ευκολότερα να αναβαθμίσουν από το αντίστοιχο GSM

Επίσης, δεδομένου ότι τα κλειδιά κρυπτογράφησης του GSM δεν ήταν ασφαλή, το UMTS πρόσθεσε έναν αλγόριθμο εμπιστευτικότητας.

Το UMTS παρέχει επίσης διαφορετικά χαρακτηριστικά γνωρίσματα ασφάλειας για τη διατήρηση της εμπιστευτικότητας ταυτότητας.

1) Η εμπιστευτικότητα της ταυτότητας των χρηστών διατηρείται με την εξασφάλιση ότι η μόνιμη ταυτότητα χρηστών (IMSI) ενός χρήστη που χρησιμοποιεί την υπηρεσία δεν μπορεί να κρυφακουστεί στην ασύρματη σύνδεση.
2) Η εμπιστευτικότητα της θέσης των χρηστών σημαίνει ότι κανένας δεν μπορεί να καθορίσει τη θέση ενός χρήστη με το να κρυφακούσει την ασύρματη σύνδεση πρόσβασης.
3) Ο μη-εντοπισμός των χρηστών εξασφαλίζει ότι δεν μπορεί να καθοριστεί εάν οι διαφορετικές υπηρεσίες είναι διαθέσιμες στον ίδιο χρήστη με το να κρυφακούσουν την ασύρματη σύνδεση πρόσβασης.

Το UMTS καυχιέται πολλά πλεονεκτήματα ασφάλειας έναντι του GSM συμπεριλαμβανομένου ενός μηχανισμού ακεραιότητας στοιχείων, μιας ενισχυμένης αυθεντικοποίησης και κρυπτογράφησης, μιας εμπιστευτικότητας ταυτότητας, μιας δυνατότητας για την ασφαλή περιπλάνηση και των μεγαλύτερων εγκαταστάσεων για την αναβάθμιση. Εντούτοις το UMTS έχει επίσης και προβλήματα ασφάλειας. Παραδείγματος χάριν όλα που θα μπορούσαν να συμβούν σε έναν σταθερό host που συνδέθηκε με το Διαδίκτυο θα μπορούσαν επίσης να συμβούν σε ένα τερματικό UMTS. Επίσης εάν η κρυπτογράφηση είναι εκτός λειτουργίας η πειρατεία των κλήσεων είναι δυνατή. Και εάν ο χρήστης σύρεται σε έναν ψεύτικο σταθμό βάσεων (base station), είναι απρόσιτος από τα σήματα σελιδοποίησης του δικτύου στο οποίο ανήκει (serving network). Τέλος όταν ο χρήστης καταχωρείτε για πρώτη φορά στο δίκτυο(serving network) η μόνιμη ταυτότητα χρηστών (IMSI) στέλνεται με απλό κείμενο.

1.8 Αρχιτεκτονικές Αλλαγές του UMTS και Νέες Υπηρεσίες

1.8.1 UMTS Έκδοση 99

Η εισαγωγή των 3G κινητών συστημάτων με το UMTS έχει απαιτήσει την εγκατάσταση ενός απολύτως νέου ασύρματου υποσυστήματος, του UMTS Radio Access Network (UTRAN). Το κεντρικό δίκτυο του UMTS είναι βασισμένο στην ίδια τεχνολογία με το GSS, με πρόσθετους όμως εξοπλισμούς (όπως οι πύλες πολυμέσων, (multimedia gateways -MGs), για τη διασύνδεση των packet and circuit switched δικτύων, που επιτρέπουν τη σύγκλιση των υπηρεσιών που βασίζονται σε αυτές τις δύο διαφορετικές τεχνικές).

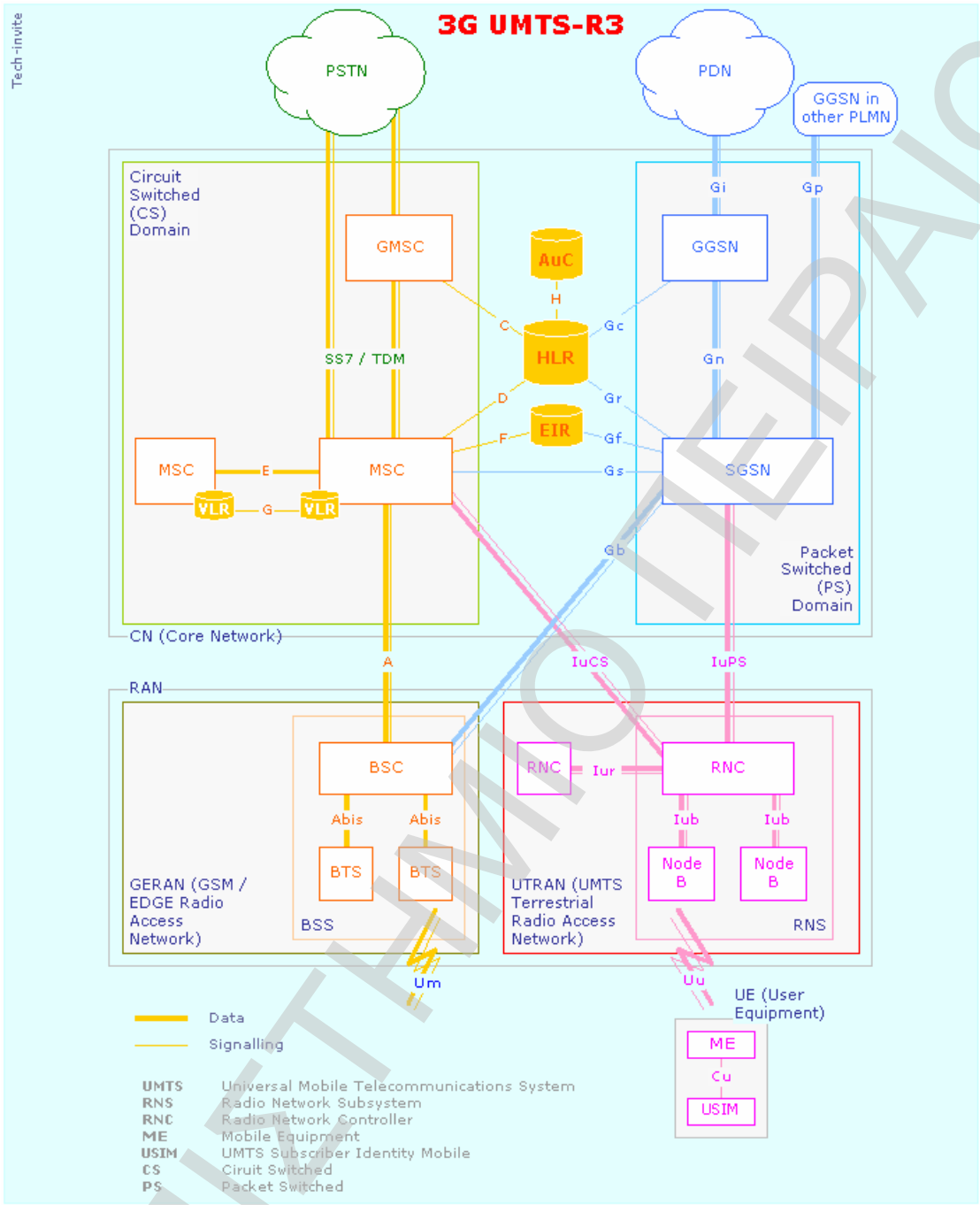
Η πρώτη έκδοση του UMTS αυξάνει το data bit rate στην ασύρματη διεπαφή έτσι ώστε υπηρεσίες πολυμέσων, όπως πχ η βιντεοκλήση, να μπορούν να προταθούν στους συνδρομητές. Το μεταβλητά data bit rate στην ασύρματη διεπαφή είναι ένα άλλο πλεονέκτημα που προσφέρεται από το UMTS έναντι του 2 και 2.5G.

Τα κύρια συστατικά ενός δικτύου UMTS είναι:

• Εξοπλισμός χρηστών (UE - User Equipment), ο οποίος περιλαμβάνει δύο μέρη: ο κινητός εξοπλισμός (ME), που είναι ένα ασύρματο τερματικό που χειρίζεται την επικοινωνία σχετικά με τη διεπαφή Uu (Uu interface) και το UMTS Subscriber Identity Module (USIM), η οποία είναι μια έξυπνη κάρτα συμπεριλαμβανομένων των στοιχείων χρηστών - ταυτότητα, αλγόριθμους αυθεντικοποίησης και πληροφορίες συνδρομής.
• Το Radio Network Controller (RNC), είναι το αντίστοιχο του BSC στο GSM. Ελέγχει τους ασύρματους πόρους (radio resource), μέσα στη σχετική κάλυψή του, μέσω των κόμβων B (nodes B).
• Ο κόμβος B (Node B), αντίστοιχο του σταθμού πομποδεκτών βάσεων GSM (BTS), μετατρέπει τις ροές δεδομένων μέσω των διεπαφών Iub και Uu. Ο ρόλος του είναι κυρίως να εκτελέσει τις λειτουργίες του physical layer (διαμόρφωση, κωδικοποίηση, προσαρμογή ποσοστού, διάδοση, κ.λπ.).
• Κεντρικό δίκτυο (Core Network) - συλλέγει όλα τα πρωτόκολλα δικτύων (για την καθιέρωση και το χειρισμό κλήσης, τη μετάδοση στοιχείων, τη διαχείριση

κινητικότητας, κ.λπ.). Δύο στρώματα καθορίζονται το Radio Network Layer και το Transport Network Layer.

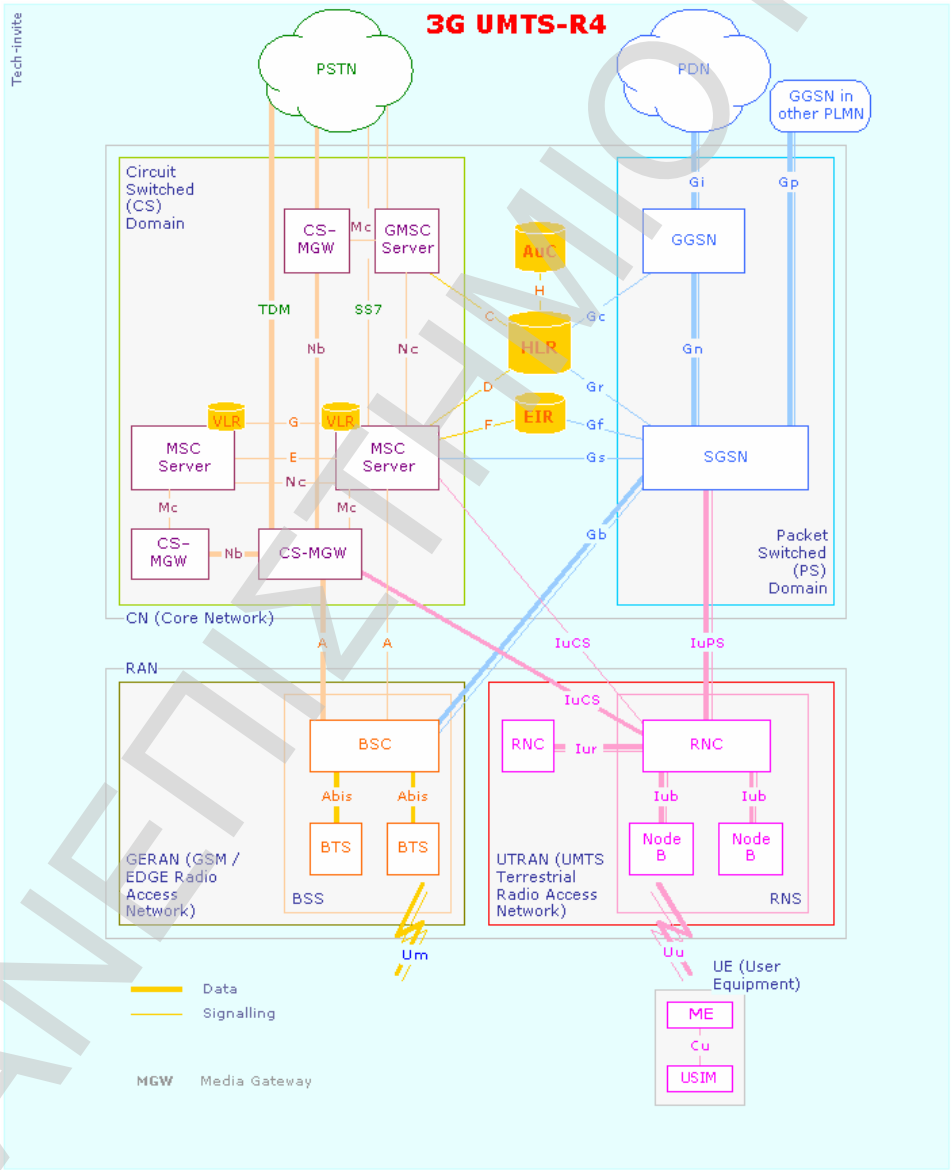
Τα μέγιστα bit rates που λαμβάνονται στα πειράματα δείχνουν ότι ένας κόμβος Β μπορεί να χειριστεί (σε ιδανικές συνθήκες) το πολύ τρεις ταυτόχρονους χρήστες βιντεοκλήσεων σε έναν ενιαίο μεταφορέα UMTS, ο οποίος είναι τρεις φορές το 384kb/s για γύρω από το εύρος ζώνης των 5MHz.



Με την Release 3 (UMTS 1) ένα νέο ασύρματο δίκτυο πρόσβασης (radio access network) αποκαλούμενο UTRAN (UMTS Terrestrial Radio Access Network) εισάγεται, βασισμένος σε W- CDMA αντί TDMA/FDMA) μετάδοση διεπαφών αέρα.

1.8.2 UMTS Έκδοση 4

Στην ακόλουθη φάση εξέλιξης του UMTS, το ασύρματο μέρος παραμένει βασικά αμετάβλητο. Στο επίπεδο κεντρικών δικτύων, το mobile switching centre (Msc) και ο κατάλογος θέσης επισκεπτών (visitor location register , VLR) γίνεται MSC servers και MGs. Οι MSC servers διαχειρίζονται τις επικοινωνίες και την κινητικότητα χρηστών και τα MGs είναι αρμόδια για τις λειτουργίες δρομολόγησης. Ο MSC server μπορεί να διαχειριστεί πολλά MG, το οποίο επιτρέπει έναν καλύτερο χωρισμό μεταξύ των λειτουργιών ελέγχου και των λειτουργιών δρομολόγησης. Αυτή η εξέλιξη επιτρέπει έναν καλύτερο χωρισμό μεταξύ των λειτουργιών ελέγχου και επεξεργασίας στο δίκτυο. Επομένως διευκολύνει την εισαγωγή των νέων χαρακτηριστικών γνωρισμάτων και συνεπώς τις νέες υπηρεσίες.



Με την Release 4, η λειτουργία του MSC είναι χωρισμένη σε δύο οντότητες:

- Ο MSC Server, ο οποίος παρέχει τα control functions
- Ο Media Gateway (MGW) server παρέχει τις λειτουργίες μετατροπής και, εάν είναι απαραίτητο, τα functions μετατροπής μεταξύ δύο διαφορετικών format. Ένας MSC Server μπορεί να ελέγξει πολλαπλάσια MGWs.

1.8.3 UMTS Έκδοση 5

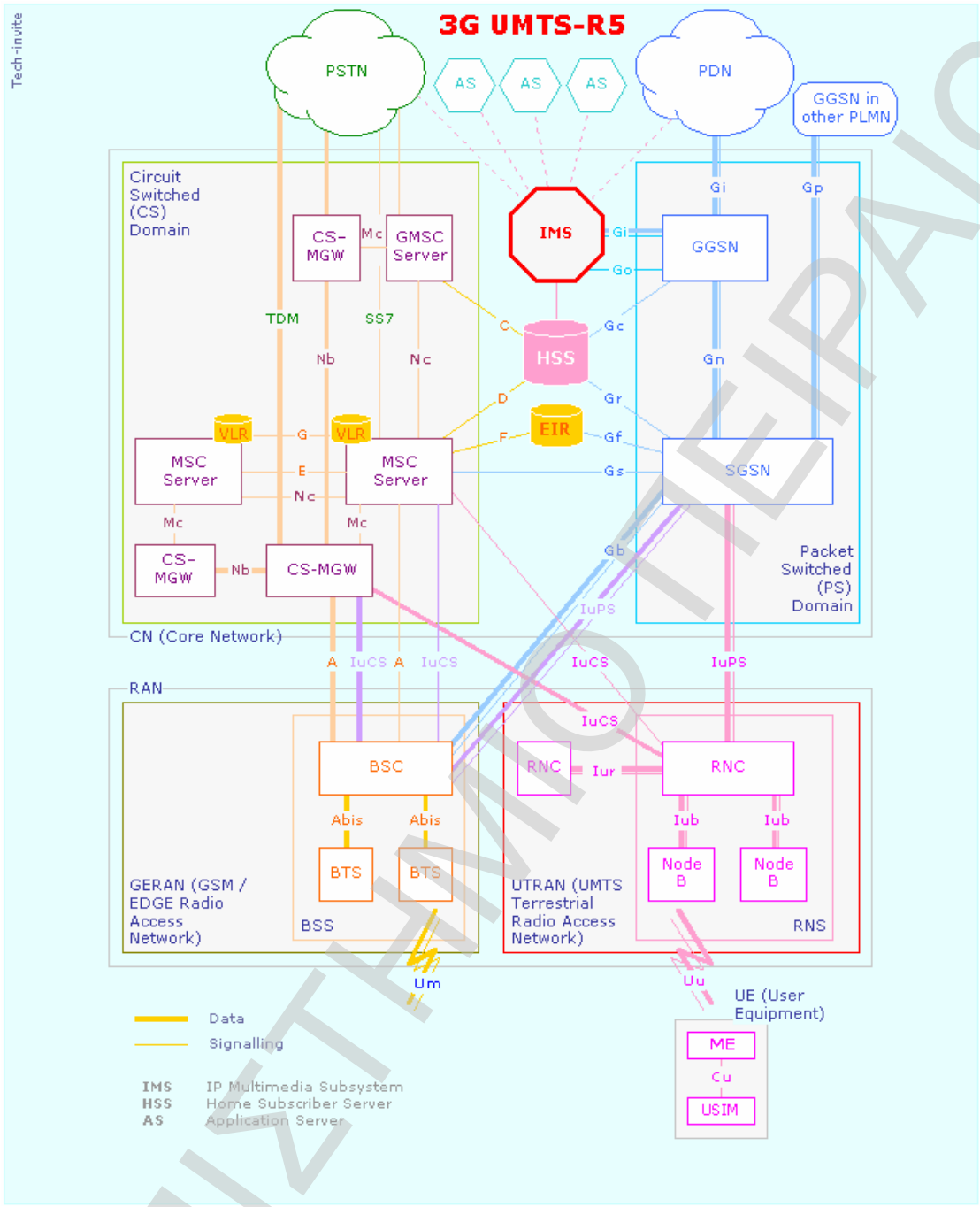
Το release 5 των προδιαγραφών UMTS είναι ένα κρίσιμο βήμα προς την ανάπτυξη και την εφαρμογή των υπηρεσιών στο περιβάλλον της κινητής τηλεφωνίας. Κατ' αρχάς, η τεχνική High-speed Downlink Packet Access (HSDPA) επιτρέπει μια σημαντική αύξηση του bit rate καθώς είναι δυνατό να επιτευχθούν πολλά Mbits το δευτερόλεπτο (μέχρι 14) σε downlink channel συνδέσεις. Οι υπηρεσίες όπως το σε πραγματικό χρόνο βίντεο, η πρόσβαση Ιστού και το FTP, κ.λπ. θα λάβουν τις βελτιωμένες ρυθμοαποδόσεις (throughputs) και, επομένως, ο τελικός χρήστης αντιλαμβάνεται την ποιότητα της υπηρεσίας. Το HSDPA επιτυγχάνεται κυρίως από τις τροποποιήσεις στο ασύρματο υποσύστημα. Στο επίπεδο δικτύων, η σημαντικότερη εξέλιξη που εισάγεται στο UMTS R5 είναι το υποσύστημα πολυμέσων IP (IMS, Multimedia subsystem), το οποίο φέρνει στους πάροχους τα μέσα για να διευκολύνει την εισαγωγή των νέων υπηρεσιών και των εφαρμογών πολυμέσων. Το IMS είναι ένα υποσύστημα που ελέγχει την παροχή υπηρεσιών μεταξύ των κεντρικών υπολογιστών (servers) και του κεντρικού δικτύου (core network). Επιτρέπει την ολοκλήρωση των σε πραγματικό χρόνο εφαρμογών και των υπηρεσιών. Τέλος, το UMTS R5 εισάγει την IP στο ασύρματο υποσύστημα (IP UTRAN) που γενικεύει τη χρήση της IP σε ολόκληρο το δίκτυο (UTRAN and core network).

Τα κύρια στοιχεία του IMS είναι τα ακόλουθα.

- Call Status Control Function (S-CSCF) ελέγχει τις κυκλοφοριακές ροές IP (IP traffic flows), κλήσεις και συνόδους (calls and sessions), και ότι συσχετίζεται με τη λειτουργία προστιθεμένης αξίας υπηρεσιών (value-added services)
- SIP Application Server (SIP AS) μπορεί να προγραμματιστεί μέσω scripts (SIP-CGI or APIs) για το VAS.

- Open Service Architecture (OSA) Service Capability Server (SCS) αντιπροσώπευση ενός ή περισσότερων χαρακτηριστικών γνωρισμάτων OSA (SCF, Service Capability Features).
- Inter-working Module (IM-SSF) SIP – CAMEL interworking module.
- Camel Service Environment (CSE) SCP χρησιμοποίηση των χαρακτηριστικών γνωρισμάτων του CAMEL και του GSM.
- Home Subscriber Server (HSS) είναι το ίδιο με το HLR σε ένα IMS περιβάλλον. Περιλαμβάνει τα στοιχεία IMS για την επικύρωση και την καθιέρωση συνόδου.

Επομένως, το IMS είναι μια νέα περιοχή(domain) που επιτρέπει τη σύγκλιση μεταξύ των σταθερών και κινητών δικτύων. Διαχειρίζεται όλες τις υπηρεσίες (υπάρχουσες υπηρεσίες, όπως circuit switched voice, voice-over IP, κ.λπ.). Το IMS είναι ένας μέσος όρος για τους πάροχους για να αναπτύξει και να εφαρμόσει τις νέες υπηρεσίες και να ενσωματώσει τον κόσμο του Διαδικτύου και επομένως όλη την σχετική επιχείρηση. Το άλλο κύριο πλεονέκτημα του IMS είναι οι προσδοκίες από την άποψη της αποταμίευσης OPEX (OPEX savings). Το IMS έχει δύο κύρια κίνητρα: οι υπηρεσίες, και το πρότυπο των πάροχων να μην καταλήγει ως bit pipe ή ISP. Οι πρώτες εφαρμογές που δοκιμάστηκαν με το IMS είναι τα στιγμιαίο μήνυμα (instant messaging), τηλεοπτική-διανομή(video-sharing) και το σε πραγματικό χρόνο τυχερό παιχνίδι (realtime gaming). Άλλες εφαρμογές, όπως το Pushto- Talk, θεωρείται επίσης υποψήφιο για να εφαρμοστεί χρησιμοποιώντας το IMS



1.8.4 UMTS Έκδοση 6

Η φανταστική αύξηση των ασύρματων δικτύων τοπικής περιοχής (LANs) στα τελευταία έτη έχει παρακινήσει τους πάροχους να ενσωματώσουν αυτήν την νέα τεχνολογία στις δραστηριότητες και τα επιχειρησιακά πρότυπά τους. Η χρήση αυτής της τεχνολογίας στην πρόσβαση στο Διαδίκτυο και των βασισμένων στην IP

υπηρεσιών και των εφαρμογών, ειδικά για τους εσωτερικούς χρήστες και τους αστικούς υπαίθριους χρήστες (low mobility urban outdoor users), είναι ένα σημαντικό κίνητρο για τους πάροχους να ενδιαφερθούν για αυτήν την σχετική με τον υπολογιστή τεχνολογία. Το Release 6 UMTS εξετάζει τα WLANs ως τμήμα ολόκληρου του δικτύου. Μέσω ενός πλουσιότερου IMS (από την άποψη των χαρακτηριστικών γνωρισμάτων) θα είναι σε θέση να διαχειριστεί τις end-to-end επικοινωνίες σχετικά με σταθερά, κινητά και WLANs δίκτυα, με βελτιώσεις στην ποιότητα της υπηρεσίας και του IMS που εφαρμόζονται στα σταθερά δίκτυα.

1.9 Πέρα από το 3G Αρχιτεκτονική (Beyond 3G Architecture)

Το 4G (που είναι γνωστό επίσης σαν beyond 3G), είναι ένα αρκτικόλεξο για το τέταρτης γενεάς σύστημα επικοινωνιών (Fourth-Generation Communications System), είναι ένας όρος που χρησιμοποιείται για να περιγράψει το επόμενο βήμα στις ασύρματες επικοινωνίες. Ένα 4G σύστημα θα είναι σε θέση να παρέχει μια περιεκτική λύση IP όπου η φωνή, τα δεδομένα και τα πολυμέσα μπορούν να δοθούν στους χρήστες "οποτεδήποτε, οπουδήποτε" (Anytime, Anywhere), και σε υψηλότερα data rates από τις προηγούμενες γενεές. Δεν υπάρχει κανένας επίσημος καθορισμός για το τι το 4G είναι, εντούτοις, υπάρχουν ορισμένοι στόχοι που προβάλλονται για το 4G.

Αυτοί οι στόχοι περιλαμβάνουν: ότι το 4G θα είναι ένα πλήρως βασισμένο σε IP ενσωματωμένο σύστημα (IP-based integrated system). Αυτό θα επιτευχθεί αφότου συγκλίνουν οι ενσύρματες και ασύρματες τεχνολογίες και θα είναι σε θέση να δώσουν 100 Mbit/s και 1 Gbit/s ταχύτητα και στο εσωτερικό και σε εξωτερικούς χώρους, με την εξαιρετική ποιότητα και την υψηλή ασφάλεια. Το 4G θα προσφέρει όλους τους τύπους υπηρεσιών με προσιτό κόστος.

Το 4G θα τροφοδοτηθεί από μια πλήρη επανάσταση στην ασύρματη τεχνολογία που στοχεύει στο καλύτερο πακετάρισμα των πληροφοριών (packing information more efficiently) για τα λιγοστά και ακριβά κύματα αέρα. Η υψηλή φασματική αποδοτικότητα (High spectral efficiency) γίνεται πιθανή, με μια 4G τεχνολογία, το Orthogonal Frequency Division Multiplexing (OFDM). Μια άλλη καινοτόμος τεχνική

που παρέχει έναν φοβερό συνδυασμό για το 4G και την ασύρματη πρόσβαση είναι η Multiple Input Multiple Output (MIMO) τεχνολογία. Με το MIMO, το BTS έχει τη νοημοσύνη για να ωθήσει περαιτέρω την ικανότητα και την κάλυψη και την ταχύτητα, καθώς χρησιμοποιεί διάφορους αλγορίθμους που εκμεταλλεύονται το κινητό περιβάλλον για να παρέχουν μια πιο καλή εμπειρία χρηστών (multi-megabit-per-second user experience). Από την πλευρά των κεντρικών δικτύων (core network), το 4G συνδυάζει πολλές από τις λειτουργίες δρομολόγησης και διαχείρισης κινητικότητας για να παραδώσει μια επίπεδη δικτυακή αρχιτεκτονική IP (flat all-IP network architecture) που ενισχύει την απόδοση των δεδομένων και μειώνει τις λειτουργικές δαπάνες.

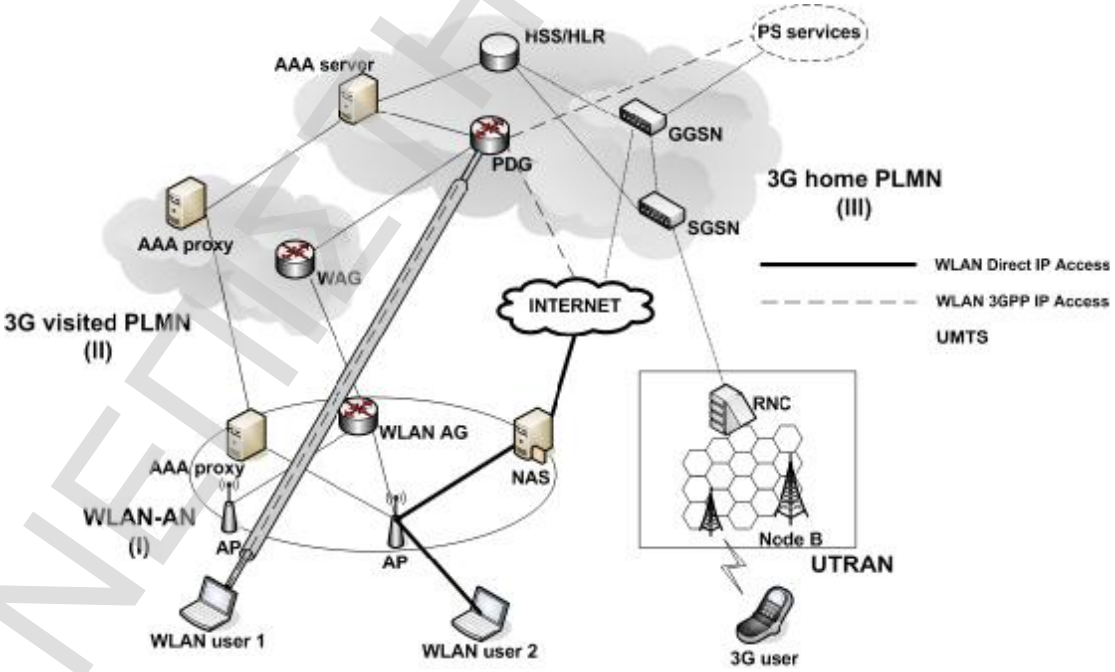
Οι νέες πεινασμένες για ταχύτητα εφαρμογές και οι σε πραγματικό χρόνο ευαίσθητες υπηρεσίες θα οδηγήσουν τη μεγαλύτερη καταναλωτική υιοθέτηση στην αγορά, και η νέα γενεά των καταναλωτικών συσκευών και των προόδων στις τρέχουσες συσκευές οδηγεί στην υπερδιασύνδεση (hyperconnectivity) - μια κατάσταση της αυξανόμενης διείσδυσης όπου κάθε χρήστης έχει τις πολλαπλάσιες συνδεδεμένες συσκευές. Το 4G κινητό broadband θα παράσχει μια βελτίωση στην απόδοση, το συνολικό κόστος της ιδιοκτησίας και τον αριθμό συσκευών που υποστηρίζονται από το δίκτυο. Αυτές οι βελτιώσεις είναι σημαντικές και θα κάνουν το 4G κινητό broadband μια αληθινά αποδιοργανωτική και επιχειρησιακά μεταβαλλόμενη τεχνολογία.

Η εξέλιξη και η επιτυχής επέκταση των ασύρματων δικτύων τοπικής περιοχής (WLANs) παγκοσμίως έχουν παραγάγει μια απαίτηση για να τα ενσωματώσουν με τα κινητά δίκτυα τρίτος-γενιάς (3G). Ο βασικός στόχος αυτής της ολοκλήρωσης είναι να αναπτυχθούν τα ετερογενή κινητά δίκτυα δεδομένων ικανά για τις νέες αναδυόμενες υπηρεσίες δεδομένων, οι οποίες απαιτούν υψηλά data rates. Η προσπάθεια να αναπτυχθούν τέτοια ετερογενή δίκτυα, που αναφέρονται επίσης όπως και πέρα από 3G (B3G) κινητά δίκτυα, υλοποιεί το όραμα για τα ασύρματα συστήματα επόμενης γενεάς, τα οποία υπόσχονται να παρέχουν την παντού και πάντα υπολογιστική δύναμη στους τελικούς χρήστες.

Όπως φαίνεται στο σχήμα πιο κάτω, η B3G δικτυακή αρχιτεκτονική αποτελείται από τρία μεμονωμένα μέρη: (I) το δίκτυο πρόσβασης WLAN (WLAN-AN), (II) το επισκεπτόμενο 3G PLMN, και (III) το τοπικό(home) 3G PLMN. Σημειώστε ότι ο αριθμός επεξηγεί την αρχιτεκτονική για μια γενική περίπτωση όπου το WLAN δεν συνδέεται άμεσα με το home 3G PLMN του χρήστη. Το WLAN-AN αποτελείται από τα ασύρματα σημεία πρόσβασης (Access Points, APs), τα οποία ενεργούν όπως την επικύρωση, έγκριση, και υπολογισμό (Authentication, Authorization, Accounting) των πελατών, που προωθούν τα σχετικά με την ασφάλεια μηνύματα στον κεντρικό υπολογιστή (AAA server) μέσω των AAA proxies, ο κεντρικός υπολογιστής πρόσβασης στο δίκτυο (Network Access Server, NAS) που παρέχει στους κινητούς χρήστες την πρόσβαση στο δημόσιο Διαδίκτυο, και η πύλη WLAN-Access Gateway (WLAN-AG) που είναι μια πύλη 3G στα δίκτυα PLMN. Υποτίθεται ότι το WLAN είναι βασισμένο στα IEEE 802.11 πρότυπα.

Αφ' ετέρου, το επισκεπτόμενο 3G PLMN περιλαμβάνει ένα AAA proxy που προωθεί τις AAA πληροφορίες στον AAA server (που βρίσκετε στο home 3G PLMN) και μια ασύρματη πύλη πρόσβασης (Wireless Access Gateway, WAG), η οποία είναι μια πύλη δεδομένων που καθοδηγεί τα δεδομένα των χρηστών στο home 3G PLMN. Τέλος, το home 3G PLMN περιλαμβάνει τον AAA server που παρέχει τις υπηρεσίες αυθεντικοποίησης στο WLAN, το Packed Data Gateway (PDG) τα μέρη του core network που αφορούν το Universal Mobile Telecommunications System (UMTS), όπως η υπηρεσία εγχώριων συνδρομητών (Home Subscriber Service ,HSS) ή ο κατάλογος εγχώριας θέσης (Home Location Register ,HLR), το κέντρο αυθεντικοποίησης (Authentication Centre ,AuC), ο κόμβος υποστήριξης πυλών GPRS (Gateway GPRS Support Node, GGSN) και ο εξυπηρετητής κόμβος υποστήριξης GPRS (Serving GPRS Support Node, SGSN). Ο AAA server ανακτά τις πληροφορίες αυθεντικοποίησης από το HSS/HLR και επικυρώνει τα πιστοποιητικά αυθεντικοποίησης(authentication credentials) που παρέχονται από τους χρήστες. Το PDG αναλαμβάνει την δρομολόγηση των δεδομένων μεταξύ ενός χρήστη και ενός εξωτερικού δικτύου δεδομένων πακέτων (external packet data network), το οποίο επιλέγεται βασισμένο στις 3G PS -υπηρεσίες που καλούνται από το χρήστη. Το τελευταίο προσδιορίζει αυτές τις υπηρεσίες με τα μέσα ενός WLAN-Access Point Name (W- APN), το οποίο αντιπροσωπεύει ένα σημείο αναφοράς στο εξωτερικό δίκτυο IP που υποστηρίζει τις υπηρεσίες PS που προσεγγίζονται από το χρήστη.

Όπως αναφέρεται προηγουμένως, η ενσωματωμένη αρχιτεκτονική B3G των δικτύων διευκρινίζει δύο διαφορετικά σενάρια πρόσβασης στο δίκτυο: (α) η άμεση IP πρόσβαση WLAN (WLAN Direct IP Access) και (β) η πρόσβαση WLAN 3GPP IP. Το πρώτο σενάριο παρέχει σε έναν χρήστη τη σύνδεση στο δημόσιο Διαδίκτυο ή σε ένα intranet μέσω WLAN-AN. Σε αυτό το σενάριο και ο χρήστης και το δίκτυο επικυρώνονται ο ένας στον άλλο χρησιμοποιώντας το EAP-SIM ή το πρωτόκολλο EAP-AKA. Επιπλέον, σε αυτό το σενάριο, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων των χρηστών που μεταφέρονται πέρα από τη διεπαφή αέρα εξασφαλίζονται από το πλαίσιο ασφάλειας 802.11i. Από την άλλη, το σενάριο πρόσβασης WLAN 3GPP IP επιτρέπει σε έναν χρήστη για συνδεθεί με τις υπηρεσίες PS (όπως WAP, mms, LBS, κ.λπ.) ή στο δημόσιο Διαδίκτυο μέσω του 3G PLMN. Σε αυτό το σενάριο, ο χρήστης επικυρώνεται στο 3G PLMN χρησιμοποιώντας το EAP-SIM ή εναλλακτικά το πρωτόκολλο EAP-AKA που τοποθετείται(encapsulated) μέσα στα μηνύματα IKEv2. Η εκτέλεση του IKEv2 χρησιμοποιείται επίσης για την καθιέρωση μιας IPsec-based VPN tunnel μεταξύ του χρήστη και του PDG που παρέχει τις υπηρεσίες εμπιστευτικότητας και ακεραιότητας στα στοιχεία που ανταλλάσσονται μεταξύ τους.

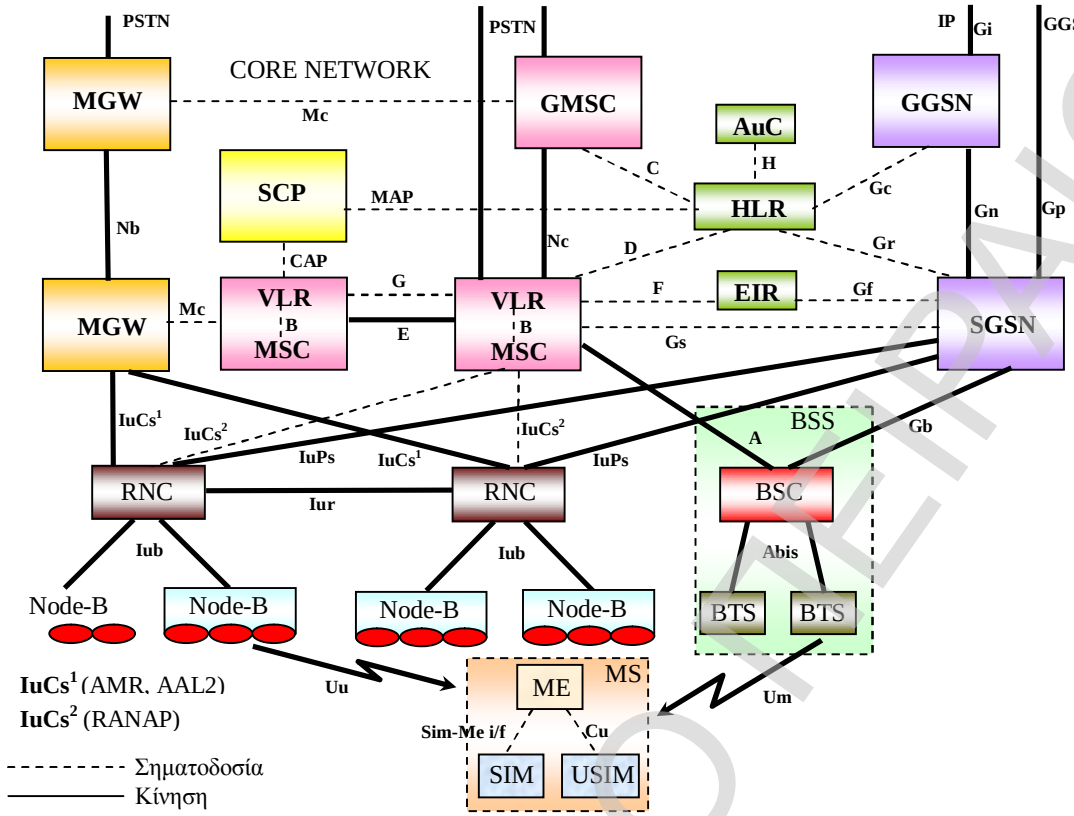


B3G δικτυακή αρχιτεκτονική

1.10 UMTS και GSM Αρχιτεκτονική ενός Παρόχου Κινητής Τηλεφωνίας (Cosmote- Ericsson)

Παρακάτω υπάρχει η τοπολογία του δικτύου UMTS και GSM του μεγαλύτερου παρόχου κινητής τηλεφωνίας της Ελλάδας, της Cosmote. Η Cosmote προώθησε τις 3G υπηρεσίες στους εταιρικούς και λιανικούς πελάτες της στης 26 Μαΐου του 2004, και έγινε ο πρώτος πάροχος στην ελληνική αγορά κινητής τηλεφωνίας που παρέχει την τηλεοπτική ροή (video streaming) , μια υπηρεσία που επιτρέπει στους πελάτες της για να απολαύσουν υψηλής ποιότητας video clips με υψηλή ταχύτητα. Η σειρά των 3G υπηρεσιών της Cosmote χαρακτηρίζει επίσης τη βίντεο-κλήση (video calling), μια υπηρεσία μέσω της οποίας οι πελάτες της Cosmote μπορούν να δουν το πρόσωπο που μιλούν κάνοντας μια κλήση, σε πραγματικό χρόνο. Εκτός από την εισαγωγή των νέων υπηρεσιών, το δίκτυο 3G της Cosmote επιτρέπει στην επιχείρηση να αναβαθμίσει τις υπάρχουσες υπηρεσίες, παρέχοντας γρηγορότερο browsing στο Διαδικτύου, την υπηρεσία μηνύματος πολυμέσων (mms) και την πρόσβαση σε ιστοσελίδες WAP με υψηλότερη ταχύτητα και πλουσιότερο περιεχόμενο.

Η Cosmote επέλεξε την Ericsson για να παραδώσει την υποδομή δικτύων συμπεριλαμβανομένου του εξοπλισμού (core and radio equipment) και για να υποστηρίξει το 3G με μια πλήρη σειρά των υπηρεσιών.



Cosmote δικτυακή αρχιτεκτονική

ΚΕΦΑΛΑΙΟ 2 : ΑΣΦΑΛΕΙΑ ΣΤΑ ΔΙΚΤΥΑ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ ΤΡΙΤΗΣ ΓΕΝΙΑΣ

2. Ασφάλεια στα Δίκτυα Κινητής Τηλεφωνίας Τρίτης Γενιάς (UMTS)

Η προστασία ασφάλειας στα 3G -δίκτυα απαιτεί την εκτίμηση διάφορων πτυχών και θεμάτων, όπως η ασύρματη πρόσβαση, την κινητικότητα των χρηστών, τις ιδιαίτερες απειλές ασφάλειας, το είδος πληροφοριών που προστατεύονται και την πολυπλοκότητα της δικτυακής αρχιτεκτονικής. Η ασύρματη μετάδοση είναι από τη φύση πιο ευαίσθητη να κρυφακουστεί από τη μετάδοση μέσω των γραμμών καλωδίων. Η κινητικότητα των χρηστών(user mobility) και η καθολική πρόσβαση στο δίκτυο προκαλούν βεβαίως απειλές στην ασφάλεια. Οι διαφορετικοί τύποι δεδομένων, όπως τα δεδομένα χρηστών, τα δεδομένα χρέωσης και τιμολόγησης, τα δεδομένα πληροφοριών πελατών και τα στοιχεία διαχείρισης των δικτύων, που μεταβιβάζονται ή κατοικούν στα δίκτυα κινητής τηλεφωνίας, απαιτούν διαφορετικό τύπο και επίπεδο προστασίας. Επιπλέον, οι σύνθετες τοπολογίες δικτύων και η ετερογένεια των περιληφθεισών τεχνολογιών αυξάνουν την πρόκληση αξιοπιστίας.

Τα κύρια στοιχεία ασφάλειας που είναι από το GSM:

- Αυθεντικοποίηση των συνδρομητών
- Εμπιστευτικότητα της ταυτότητα των συνδρομητών (Subscriber identity confidentially)
- Το Subscriber Identity Module (SIM) να είναι μετακινούμενο από το τελικό υλικό (κινητό τηλέφωνο)
- Κρυπτογράφηση των ραδιο-διεπαφών (Radio interface encryption)

Πρόσθετα χαρακτηριστικά γνωρίσματα ασφάλειας στο UMTS:

- Ασφάλεια ενάντια στη χρησιμοποίηση ψεύτικων σταθμών βάσεων με την αμοιβαία επικύρωση
- Κρυπτογράφηση που επεκτείνεται στη σύνδεση RNC με τον κόμβο-Β
- Τα στοιχεία ασφάλειας στο δίκτυο θα προστατευθούν στις αποθηκεύσεις δεδομένων και θα προστατεύονται ακόμα και όταν διαβιβάζονται κλειδιά και δεδομένα αυθεντικοποίησης στο σύστημα.
- Μηχανισμός για αναβάθμιση των χαρακτηριστικών ασφάλειας.

Η κυκλοφορία των κεντρικών δικτύων(Core network traffic) μεταξύ RNCs, MSCs και άλλων δικτύων δεν είναι κρυπτογραφημένη και οι πάροχοι μπορούν να εφαρμόσουν προστασία για τις συνδέσεις μετάδοσης κεντρικών δικτύων τους, αλλά αυτό δύσκολα μπορεί να συμβεί. Τα MSCs θα έχουν από κατασκευής ικανότητες και πρόσβαση στα Call Data Records (SDR), έτσι όλα τα switches θα πρέπει να έχουν μέτρα ασφάλειας ενάντια στην παράνομη πρόσβαση.

Η προδιαγραφή UMTS έχει πέντε ομάδες χαρακτηριστικών γνωρισμάτων ασφάλειας:

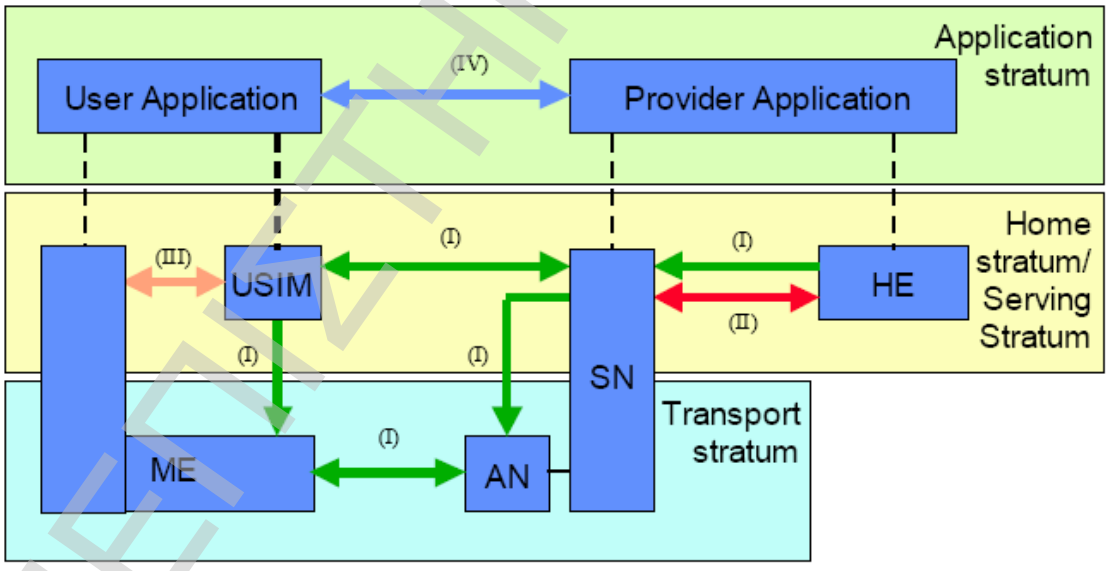
- Network access security: Αυτό το χαρακτηριστικό γνώρισμα επιτρέπει στους χρήστες για να έχουν πρόσβαση ασφαλώς στις υπηρεσίες που παρέχονται από το 3G δίκτυο. Αυτό το χαρακτηριστικό γνώρισμα είναι αρμόδιο για την παροχή της εμπιστευτικότητας ταυτότητας, της επικύρωσης των χρηστών, της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικοποίησης του κινητού εξοπλισμού. Η εμπιστευτικότητα ταυτότητας χρηστών λαμβάνεται με τη χρησιμοποίηση μιας προσωρινής ταυτότητας αποκαλούμενης ως International Mobile User Identity. Η αυθεντικοποίηση επιτυγχάνεται χρησιμοποιώντας μια μέθοδο απάντησης (challenge response method) χρησιμοποιώντας ένα μυστικό κλειδί. Η εμπιστευτικότητα λαμβάνεται με τη βοήθεια ενός μυστικού κρυπτογραφημένου κλειδιού (Cipher Key) που ανταλλάσσεται ως τμήμα της αυθεντικοποίησης και της βασικής διαδικασίας συμφωνίας (Authentication and Key Agreement Process, AKA). Η ακεραιότητα παρέχεται χρησιμοποιώντας έναν αλγόριθμο και ένα κλειδί (IK) ακεραιότητας. Ο προσδιορισμός εξοπλισμού επιτυγχάνεται χρησιμοποιώντας το International Mobile Equipment Identifier (IMEI)

- Network domain security: το σύνολο των χαρακτηριστικών γνωρισμάτων ασφάλειας που επιτρέπουν στους κόμβους στο domain του πάροχου να ανταλλάξουν ασφαλώς τα δεδομένα και να προστατευτούν από τις επιθέσεις στο ενσύρματο δίκτυο.

- User domain security: τα χαρακτηριστικά γνωρίσματα μέσα στο USIM έτσι ώστε μόνο οι εξουσιοδοτημένοι χρήστες (δηλαδή εκείνοι που ξέρουν τον προσωπικό αριθμό αναγνώρισης (PIN)) να μπορούν να έχουν πρόσβαση στο USIM και στο ME. Μερικά δεδομένα του USIM πρέπει να προστατευθούν από πρόσβαση από το χρήστη.

- Application domain security: περιλαμβάνει τους μηχανισμούς ασφάλειας για πρόσβαση στα στοιχεία παραμέτρων του χρήστη (user profile data). Μηχανισμοί ασφάλειας IP για να παρέχει ασφαλή ανταλλαγή μηνυμάτων μεταξύ του δικτύου και του USIM.

- Visibility and configurability of security: Η διαφάνεια και η δυνατότητα ρύθμισης της ασφάλειας, αυτό το χαρακτηριστικό γνώρισμα επιτρέπει στους χρήστες να ενημερωθούν εάν ένα χαρακτηριστικό γνώρισμα ασφάλειας είναι σε λειτουργία και εάν η χρήση και η λειτουργία μιας ορισμένης υπηρεσίας πρέπει να εξαρτηθεί από το χαρακτηριστικό γνώρισμα ασφάλειας.



Επισκόπηση της αρχιτεκτονικής ασφάλειας

Η προδιαγραφή του UMTS έχει τα ακόλουθα χαρακτηριστικά γνωρίσματα ασφάλειας σχετικά με την εμπιστευτικότητα της ταυτότητας των χρηστών:

- User identity confidentiality: η μόνιμη ταυτότητα χρηστών (IMSI) ενός χρήστη στον οποίο οι υπηρεσίες παραδίδονται δεν μπορεί να κρυφακουστεί στη ραδιο-σύνδεση πρόσβασης.
- User location confidentiality: η παρουσία ή η άφιξη ενός χρήστη σε μια ορισμένη περιοχή δεν μπορεί να βρεθεί με το να κρυφακούσει κάποιος στη ραδιο σύνδεση πρόσβασης.
- User un-traceability: ένας εισβολέας δεν μπορεί να συναγάγει εάν οι διαφορετικές υπηρεσίες παραδίδονται στον ίδιο χρήστη με το να κρυφακούσει στη ραδιο σύνδεση πρόσβασης.

Η ασύρματη κρυπτογράφηση/αποκρυπτογράφηση γίνετε στο RNC στην πλευρά των δικτύων και στα κινητά τερματικά. Η κρυπτογράφηση γίνετε είτε σε επίπεδο Radio Link Control (RLC) είτε σε επίπεδο Medium Access control (MAC).

2.1 Ασφάλεια Πρόσβασης στο Δίκτυο (network access security)

Η ασφάλεια πρόσβασης στο δίκτυο είναι ένα βασικό συστατικό στην αρχιτεκτονική της 3G ασφάλειας. Αυτή η κατηγορία εξετάζει το σύνολο των μηχανισμών ασφάλειας που παρέχουν στους χρήστες την ασφαλή πρόσβαση στις 3G υπηρεσίες, καθώς επίσης και προστατεύει από τις επιθέσεις στη ραδιο διεπαφή. Τέτοιοι μηχανισμοί περιλαμβάνουν:

- εμπιστευτικότητα ταυτότητας χρηστών (user identity confidentiality)
- αυθεντικοποίηση και συμφωνία για τα κλειδιά (authentication and key agreement)
- εμπιστευτικότητα δεδομένων (data confidentiality)
- προστασία ακεραιότητας των μηνυμάτων (integrity protection of signaling messages)

Η ασφάλεια πρόσβασης στο δίκτυο πραγματοποιείται ανεξάρτητα σε κάθε περιοχή (domain) υπηρεσιών.

2.1.1 Εμπιστευτικότητα Ταυτότητας Χρηστών (user identity confidentiality)

Η εμπιστευτικότητα της ταυτότητας των χρηστών επιτρέπει τον προσδιορισμό ενός χρήστη στη ραδιο-σύνδεση πρόσβασης(radio access link) με τη βοήθεια του Temporary Mobile Subscriber Identity (TMSI). Αυτό υπονοεί ότι η εμπιστευτικότητα της ταυτότητας των χρηστών προστατεύεται σχεδόν πάντα από τους παθητικούς ωτακουστές. Η αρχική εγγραφή είναι μια εξαιρετική περίπτωση όπου μια προσωρινή ταυτότητα πρέπει να χρησιμοποιηθεί, δεδομένου ότι το δίκτυο δεν ξέρει ακόμα τη μόνιμη ταυτότητα του χρήστη.

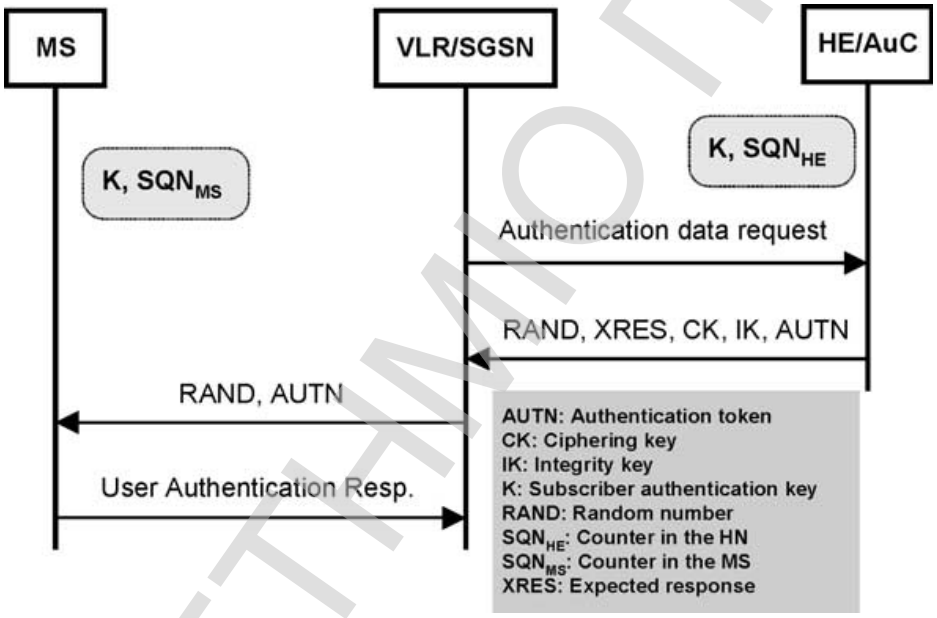
Η διατιθέμενη προσωρινή ταυτότητα μεταφέρεται στο χρήστη μόλις ανοιχτεί η κρυπτογράφηση. Ένα TMSI στο CS domain ή το P-TMSI στο PS domain έχει μια τοπική σημασία μόνο στην περιοχή θέσης ή την περιοχή δρομολόγησης, στις οποίες ο χρήστης εγγράφεται. Η ένωση μεταξύ των μόνιμων και προσωρινών ταυτοτήτων χρηστών αποθηκεύεται στο Visited Location Register ή στο Serving GPRS Support Node (VLR/SGSN). Εάν ο χρήστης φθάνει σε μια νέα περιοχή, τότε, η ένωση μεταξύ της μόνιμης και προσωρινής ταυτότητας μπορεί να προσκομιστεί από την παλαιά περιοχή θέσης ή δρομολόγησης (old location or routing area). Εάν η διεύθυνση της παλαιάς περιοχής δεν είναι γνωστή ή η σύνδεση δεν μπορεί να καθιερωθεί, κατόπιν, η μόνιμη ταυτότητα πρέπει να ζητηθεί από τον χρήστη.

Για να αποφύγει την ανιχνευσιμότητα των χρηστών(traceability), που μπορεί να οδηγήσει σε πρόβλημα της εμπιστευτικότητας της ταυτότητας των χρηστών καθώς επίσης και στον εντοπισμό της θέσης των χρηστών, ο χρήστης δεν πρέπει να προσδιοριστεί για μια μεγάλη περίοδο με τη βοήθεια της ίδιας προσωρινής ταυτότητας. Επιπλέον, οποιαδήποτε σηματοδότηση ή δεδομένα χρηστών που μπορούν να αποκαλύψουν την ταυτότητα του χρήστη κρυπτογραφούνται στη ραδιο σύνδεση πρόσβασης.

2.1.2 Αυθεντικοποίηση και Συμφωνία για τα Κλειδιά (authentication and key agreement)

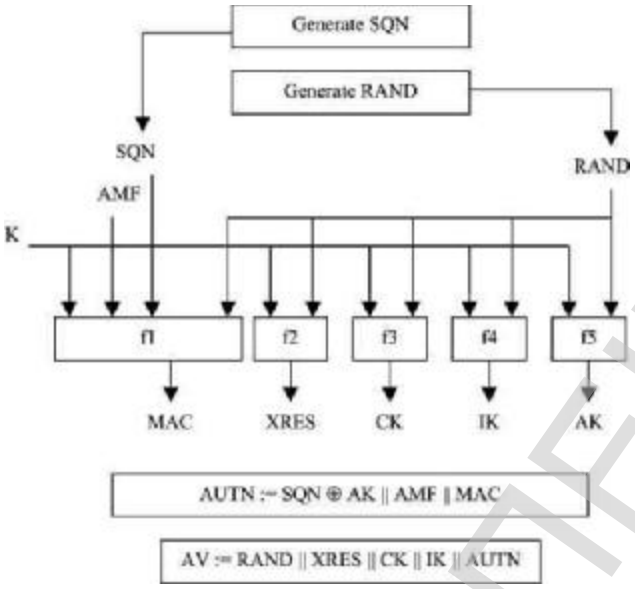
Η αυθεντικοποίηση και η συμφωνία για τα κλειδιά επιτυγχάνουν την αμοιβαία αυθεντικοποίηση μεταξύ του κινητού χρήστη και του SN έχοντας τη γνώση ενός μυστικού κλειδιού K. Το κλειδί K παράγει επίσης τα κλειδιά λογαριασμού και

αυθεντικοποίησης. Η μέθοδος αυθεντικοποίησης αποτελείται από ένα πρωτόκολλο πρόκλησης/απάντησης (challenge/response protocol) και επιλέχτηκε με τέτοιο τρόπο ώστε να επιτευχθεί η μέγιστη συμβατότητα με την αρχιτεκτονική του GSM/GPRS ασφάλειας που διευκολύνει τη μετάβαση από το GSM/GPRS στο UMTS. Επιπλέον, το User Service Identity Module (USIM) και το HE παρακολουθεί τους μετρητές SQNms και SQNhe, αντίστοιχα, για να υποστηρίξει την αυθεντικοποίηση των δικτύων. Ο αριθμός ακολουθίας SQNhe είναι ένας μεμονωμένος μετρητής για κάθε χρήστη, ενώ το SQNms δείχνει τον υψηλότερο αριθμό ακολουθίας που το USIM έχει δεχτεί



Αυθεντικοποίηση και Συμφωνία για τα Κλειδιά

Επάνω στην παραλαβή ενός αιτήματος από το VLR/SGSN, το HE κέντρο αυθεντικοποίησης (HE/AuC) προωθεί μια διαταγμένη σειρά διανυσμάτων αυθεντικοποίησης (authentication vectors, AV) επικύρωσης στο VLR/SGSN. Κάθε AV, που χρησιμοποιείται στην αυθεντικοποίηση και τη βασική διαδικασία συμφωνίας των κλειδιών μεταξύ του VLR/SGSN και του USIM, αποτελείται από ένα τυχαίο αριθμό RAND, μια αναμενόμενη απάντηση XRES, ένα κρυπτογραφημένο κλειδί CK, ένα integrity key IK και ένα authentication token AUTN.



Παραγωγή των διανυσμάτων αυθεντικοποίησης

Το HE/AuC αρχίζει με την παραγωγή ενός φρέσκου αριθμού ακολουθίας SQN, ο οποίος αποδεικνύει στο χρήστη ότι το παραγμένο AV δεν έχει χρησιμοποιηθεί πριν και ένα τυχαίο RAND. Κατόπιν, χρησιμοποιώντας το μυστικό βασικό κλειδί K υπολογίζει:

- Ο κώδικας επικύρωσης μηνυμάτων (Message Authentication Code) MAC = *f1k* (SQN|| RAND||AMF), όπου f1 είναι μια λειτουργία αυθεντικοποίησης μηνυμάτων και το Authentication and key Management Field (AMF) χρησιμοποιείται για να βελτιστοποιήσει την απόδοση ή να φέρει ένα νέο κλειδί αυθεντικοποίησης που αποθηκεύεται στο USIM σε χρήση.
- Η αναμενόμενη απάντηση XRES = *f2k* (RAND) όπου το f2 είναι μια (ενδεχομένως περικομμένη) συνάρτηση αυθεντικοποίησης μηνυμάτων.
- Το κρυπτογραφημένο κλειδί CK = *f3k* (RAND)
- Το Integrity Key IK = *f4K* (RAND)
- Το κλειδί ανωνυμίας AK= *f5K* (RAND) όπου f3, f4 και f5 είναι συναρτήσεις παραγωγής κλειδιών
- Τέλος, το HE/AuC συγκεντρώνει το authentication token AUTN = SQN ⊕ AK || AMF || MAC

Πρέπει να σημειωθεί ότι η αυθεντικοποίηση και οι βασικές λειτουργίες παραγωγής κλειδιών f1, f2, f3, f4 και f5, και ο επακόλουθος υπολογισμός του AV ακολουθούν τη μονόδρομη διαδρομή(one-way). Αυτό σημαίνει ότι εάν το αποτέλεσμα είναι γνωστό δεν υπάρχει κανένας αποδοτικός αλγόριθμος για να συναγάγετε οποιαδήποτε εισαγωγή που θα παράγει το ίδιο αποτέλεσμα. Αν και οι συναρτήσεις f1-f5 είναι βασισμένες στον ίδιο βασικό αλγόριθμο, διαφέρουν η μια από την άλλη με έναν θεμελιώδη τρόπο προκειμένου να είναι αδύνατο να συναγάγουμε οποιεσδήποτε πληροφορίες για το αποτέλεσμα μιας συνάρτησης από το αποτέλεσμα των άλλων. Δεδομένου ότι χρησιμοποιούνται στο AuC και στο USIM, το οποίο ελέγχεται από τον πάροχο (home operator), η επιλογή των αλγορίθμων (f1 - f5) είναι διαλεγμένες και μοναδικές για τον κάθε πάροχο. Εντούτοις, ένα σύνολο αλγορίθμων έχει προταθεί αποκαλούμενο ως MILENAGE.

Όταν το VLR/SGSN κινεί μια αυθεντικοποίηση και μια βασική διαδικασία συμφωνίας κλειδιών (authentication and key agreement), επιλέγει το επόμενο AV από τη διαταγμένη σειρά και προωθεί τις παραμέτρους RAND και AUTN στο χρήστη. Το USIM που χρησιμοποιεί επίσης το μυστικό βασικό κλειδί K υπολογίζει το AK,

AK= *f5K* (RAND) και ανακτά το SQN, SQN = (SQN ⊕ AK) ⊕ AK

Κατόπιν, υπολογίζει το *XMAC = f1K (SQN || RAND || AMF),* και ελέγχει εάν το λαμβανόμενο AUTN και οι ανακτημένες τιμές του SQN παρήχθησαν πράγματι στο AuC. Σε αυτή την περίπτωση, το USIM υπολογίζει το RES = *f2k* (RAND), και προκαλεί τον κινητό σταθμό (MS) για να στείλει μια απάντηση αυθεντικοποίησης χρηστών πίσω. Κατόπιν, το USIM υπολογίζει τα CK,

CK = *f3K* (RAND), και το IK, IK = *f4K* (RAND).

Το VLR/SGSN συγκρίνει το λαμβανόμενο RES με το XRES πεδίο του AV. Εάν ταιριάζουν, θεωρεί ότι η αυθεντικοποίηση και η βασική ανταλλαγή κλειδιών έχουν ολοκληρωθεί επιτυχώς. Τέλος, το USIM και το VLR/SGSN μεταφέρουν τα καθιερωμένα κλειδιά κρυπτογράφησης και κλειδιά προστασίας ακεραιότητας

(encryption and integrity protection keys) για τον κινητό εξοπλισμό και το Radio Network Controller (RNC) που εκτελούν την κρυπτογράφηση και τις συναρτήσεις ακεραιότητας (integrity functions).

2.1.3 Εμπιστευτικότητα Δεδομένων (data confidentiality)

Μόλις ο χρήστης και το δίκτυο έχει αυθεντικοποίηθεί μεταξύ τους, μπορούν να αρχίσουν μια ασφαλής επικοινωνία. Όπως περιγράφεται παρακάτω, ένα κρυπτογραφημένο κλειδί μοιράζεται μεταξύ του κεντρικού δικτύου(core network) και του τερματικού μετά από ένα επιτυχές γεγονός επικύρωσης. Τα δεδομένα του χρήστη που στέλνονται πέρα από τη ραδιο-διεπαφή υπόκεινται σε κρυπτογράφηση χρησιμοποιώντας τη συνάρτηση f8.

Η διαδικασία κρυπτογράφησης/αποκρυπτογράφησης πραγματοποιείται στο MS και το RNC από την πλευρά του δικτύου. Ο F8 είναι ένας συμμετρικός σύγχρονος αλγόριθμος κρυπτογράφησης που χρησιμοποιείται για να κρυπτογραφήσει τα πλαίσια μεταβλητού μήκους. Η κύρια είσοδος στον f8 είναι ένα 128-bit μυστικό κλειδί CK. Οι πρόσθετες είσοδοι που χρησιμοποιούνται για να εξασφαλίσουν ότι δύο πλαίσια κρυπτογραφούνται χρησιμοποιώντας τα διαφορετικά keystreams, είναι μια 32-bit COUNT, μια 5-bit BEARER και μια 1-bit DIRECTION. Η έξοδος είναι μια ακολουθία bits (keystream) του ίδιου μήκους με το πλαίσιο. Το πλαίσιο κρυπτογραφείται με XOR με τα στοιχεία του keystream. Για το UMTS R99, το f8 είναι βασισμένο στον αλγόριθμο Kasumi.

Ο αλγόριθμος Kasumi είναι ένας block cipher αλγόριθμος που λειτουργεί σε 64-bit blocks χρησιμοποιώντας ένα 128-bit κλειδί. Είναι βασισμένο σε μια δομή Feistel με 8 κύκλους (το 3DES έχει μια 48-κύκλων δομή Feistel). Ο KASUMI διευκρινίζεται στη 3GPP τεχνική προδιαγραφή TS 35.202. Η f9 συνάρτηση στο πρωτόκολλο ασφάλειας UMTS είναι μια συνάρτηση ακεραιότητας(integrity function) βασισμένη στο block cipher του KASUMI. Παράγει ένα MAC για ένα μήνυμα με τη χρησιμοποίηση του KASUMI σε CBC τρόπο λειτουργίας. Εάν ένα μήνυμα αποτελείται από q n-bit blocks D1,D2…Dq, και το Ek(X) είναι η κρυπτογράφηση του block X που χρησιμοποιεί το κλειδί K, κατόπιν η f9 MAC συνάρτηση μπορεί να περιγράφει σαν:

1) H1 = Ek(D1),

2) Hi = Ek(Di ⊕ Hi-1) και

3) MAC = Ek'(H1 ⊕ H2 ⊕…⊕ Hq).

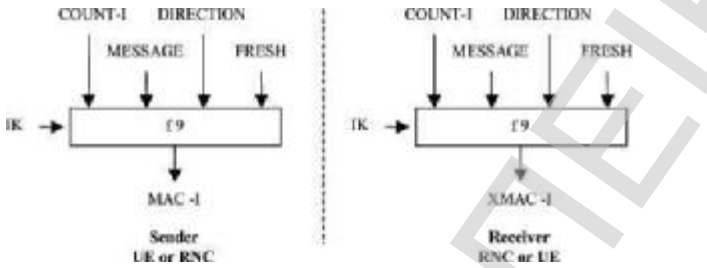
Διάφορες hardware εφαρμογές του αλγορίθμου KASUMI εξετάζονται. Για να κάνουμε μια δίκαιη σύγκριση χρησιμοποιούμε τα αποτελέσματα από την εφαρμογή του Xilinx FPGA. Η συμπαγής 2 στροφών υλοποίηση παράγει ένα throughput 167.04 Mbit/s σε μια μέγιστη συχνότητα 20,88 MHz χρησιμοποιώντας 1287 CLB slices. Η γρηγορότερη 8- round υλοποίηση έχει ένα throughput 2414.08 Mbit/s και απαιτεί 2213 CLB slices, αλλά αυτό δεν είναι στον τρόπο ανατροφοδότησης. Δυστυχώς καμία πληροφορία δεν βρίσκεται για οποιαδήποτε απόδοση λογισμικού με χρήση της f9 συνάρτησης λειτουργίας KASUMI.

2.1.4 Προστασία της Ακεραιότητας των Μηνυμάτων (integrity protection of signaling messages)

Μόλις καθιερωθεί ένα κλειδί ακεραιότητας(integrity key) ως τμήμα ενός πρωτοκόλλου αυθεντικοποίησης που υπάρχει και μόλις είναι γνωστοί οι διαθέσιμοι αλγόριθμοι προστασίας της ακεραιότητας του MS, το δίκτυο μπορεί να αρχίσει την προστασία ακεραιότητας(integrity protection). Η προστασία ακεραιότητας εφαρμόζεται στον κινητό εξοπλισμό (ME) στην πλευρά του χρήστη και στο radio network controller (RNC) στην πλευρά των δικτύων. Μια συνάρτηση επικύρωσης μηνυμάτων εφαρμόζεται σε κάθε μεμονωμένο σήμα σε επίπεδο radio resource control (RRC) στην (UMTS Terrestrial Radio Access Network) UTRAN λίστα πρωτοκόλλων (protocol stack).

Μετά από την καθιέρωση σύνδεσης RRC και την εκτέλεση της διαδικασίας ασφάλειας για την καθιέρωση μιας σύνδεσης(security mode establishment procedure), τα περισσότερα από τα επόμενα μηνύματα RRC έχουν την ακεραιότητα να προστατεύεται. Αυτό περιλαμβάνει τα RRC μηνύματα, συν τα αποκαλούμενα

άμεσα μηνύματα μεταφοράς RRC(RRC direct transfer messages), τα οποία περιέχουν και δεδομένα πρωτοκόλλου για το υψηλότερο στρώμα που αφιερώνεται επικοινωνίας μεταξύ του ΜΕ και του κεντρικού δικτύου. Η προστασία των άμεσων μηνυμάτων μεταφοράς επιτρέπει τη διαχείριση κινητικότητας, τον έλεγχο κλήσης και τη διαχείριση συνόδου να προστατευθεί.



Επεξηγεί τη χρήση του αλγορίθμου ακεραιότητας f9 για να επικυρώσει την ακεραιότητα των δεδομένων ενός μηνύματος RRC

Οι παράμετροι εισαγωγής στον αλγόριθμο είναι:

- ένα κλειδί ακεραιότητας IK(integrity key), που είναι 128 bits
- ένας αριθμός ακολουθίας ακεραιότητας (COUNT-I) και μια τυχαία μεταβλητή που παράγεται από το radio network controller (FRESH). Το COUNT-I και το FRESH είναι κάθε ένα 32 bits.

Μαζί, παρέχουν την προστασία επανάληψης (replay protection)

- ένα προσδιοριστικό κατεύθυνσης (DIRECTION) για να αποτρέψει τις αποκαλούμενες επιθέσεις αντανάκλασης(reflection attacks)
- το περιεχόμενο των μηνυμάτων RRC (MESSAGE).

Με βάση αυτές τις παραμέτρους εισαγωγής ο αποστολέας υπολογίζει τον 32 bit μήνυμα αυθεντικοποίησης για την ακεραιότητα των δεδομένων (MAC-I) χρησιμοποιώντας τον αλγόριθμο ακεραιότητας f9. Το MAC-I επισυνάπτεται έπειτα στο μήνυμα RRC όταν στέλνεται πέρα από τη ραδιο σύνδεση πρόσβασης. Ο δέκτης υπολογίζει το αναμενόμενο MAC-I (XMAC-I) στο μήνυμα που το έλαβε με τον ίδιο τρόπο όπως ο αποστολέας υπολόγισε το MAC-I στο μήνυμα που εστάλη και ελέγχει

την ακεραιότητα των δεδομένων του μηνύματος με τη σύγκριση του με το λαμβανόμενο MAC-I.

Το χαρακτηριστικό γνώρισμα της ακεραιότητας παρέχει επίσης την επικύρωση προέλευσης των δεδομένων, έτσι ώστε ο δέκτης ενός προστατευμένου μηνύματος (integrity-protected) να μπορεί να επιβεβαιώσει την ταυτότητα του αποστολέα. Αυτό επιτρέπει σε έναν πάροχο να μην τρέξει την πλήρη επικύρωση και το βασικό πρωτόκολλο συμφωνίας κάθε φορά που καθιερώνεται μια σύνδεση.

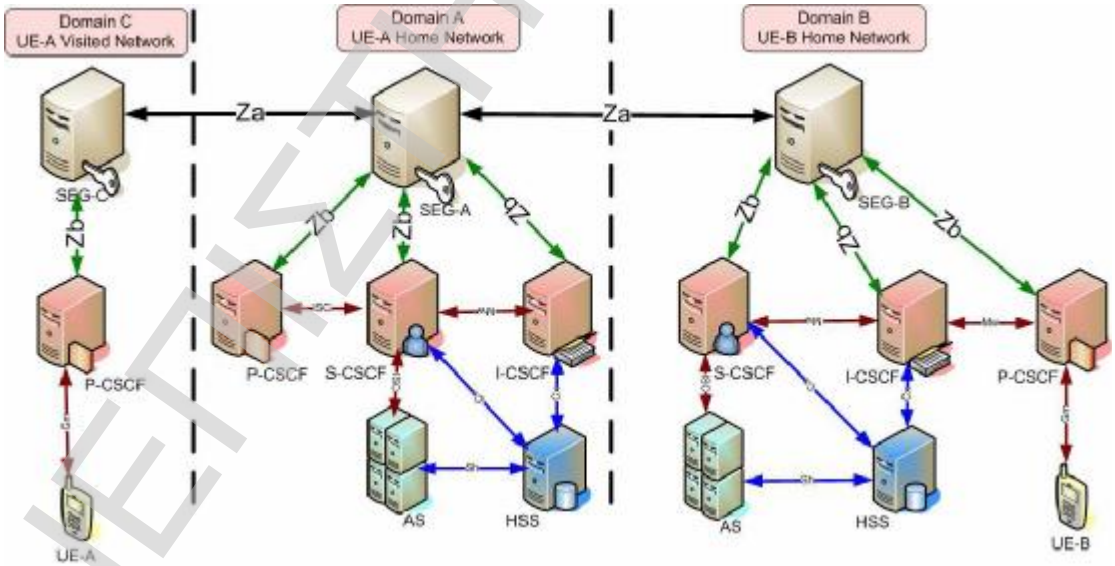
2.2 Ασφάλεια Δικτύων (network domain security)

Το domain των δικτύων είναι ένα δίκτυο που ελέγχεται από μια ενιαία αρχή χειριστών ή administrator με σκοπό να εφαρμόσει μια ομοιόμορφη πολιτική ασφάλειας μέσα στην περιοχή. Ως εκ τούτου, το επίπεδο ασφάλειας και οι διαθέσιμες υπηρεσίες ασφάλειας είναι ίδιες μέσα στην περιοχή ασφάλειας. Η ασφάλεια των δικτύων εφαρμόζεται στα όρια του δικτύου του πάροχου και προστατεύεται από τα Security Gateways (SEGs). Το NDS/IP χρησιμοποιείται για να προστατεύσει το κεντρικό δίκτυο IMS(IMS core network) του πάροχου και την κυκλοφορία μεταξύ των visited και home networks. Η θεμελιώδης ιδέα της αρχιτεκτονικής NDS/IP είναι να παρασχεθεί η hop-by-hop ασφάλεια που βοηθά να διατηρήσει χωριστές πολιτικές ασφάλειας εσωτερικά και προς άλλες εξωτερικές περιοχές ασφάλειας.

Στο NDS/IP, τα Security Gateways διατηρούν ασφαλείς IPSec ESP (Encapsulated Security Payload) Security Associations με χρήση tunnel mode ανάμεσα στα domains ασφάλειας. Όλη η κυκλοφορία NDS/IP από τις οντότητες δικτύων της περιοχής ασφάλειας(network entities of security domain) καθοδηγείται μέσω SEG σε άλλη περιοχή ασφάλειας χρησιμοποιώντας την προστασία ασφάλειας hop-by-hop μέχρι τον προορισμό.

2.2.1 Διεπαφές NDS (NDS interfaces)

Οι διεπαφές(interfaces) μεταξύ των περιοχών ασφάλειας(security domains) αντιπροσωπεύονται ως Za ενώ οι διεπαφές μέσα στην περιοχή ασφάλειας αντιπροσωπεύονται ως Zb όπως φαίνεται στο κατωτέρω σχήμα. Η διεπαφή Za καλύπτει όλη την κυκλοφορία NDS/IP μεταξύ των περιοχών ασφάλειας. Για την Za -διεπαφή, η αυθεντικοποίηση και η προστασία ακεραιότητας των δεδομένων απαιτείτε και η κρυπτογράφηση στοιχείων συστήνεται. Αυτά τα τρία χαρακτηριστικά γνωρίσματα ασφάλειας εφαρμόζονται με το να χρησιμοποιήσουν το ESP (Encapsulated Security Payload) πρωτόκολλο. Τα SEGs χρησημοποιούν το IKE (Internet Key Exchange) για να διαπραγματευτούν, να καθιερώσουν και να διατηρήσουν ένα ασφαλές ESP tunnel για της προωθηση της NDS/IP κυκλοφορίας μεταξύ των περιοχών ασφάλειας. Η πολιτική ασφάλειας πέρα από την Za -διεπαφή εξαρτάται από τη συμφωνία roaming. Για την Zb -διεπαφή, η αυθεντικοποίηση και η προστασία ακεραιότητας των δεδομένων απαιτείτε και εφαρμόζετε με χρήση του ESP πρωτόκολλου. Η κρυπτογράφηση στοιχείων είναι προαιρετική και εξαρτάται από την απόφαση του χειριστή των περιοχών ασφάλειας.



Inter-Domains Security Architecture

2.2.2 Πύλες Ασφάλειας (security gateways, SEGs)

Οι πύλες ασφάλειας(Security Gateways) είναι οντότητες δικτύων στα σύνορα των περιοχών ασφάλειας IP(IP security domains), που παρέχουν την ασφάλεια βασισμένη στα IP πρωτόκολλα και καθιερώνουν την επικοινωνία πέρα από τη διεπαφή Za. Όλη η κυκλοφορία NDS/IP περνά μέσω SEG πριν μπει ή αφήσει την περιοχή ασφάλειας. Μια περιοχή ασφάλειας μπορεί να έχει περισσότερα από ένα SEG ανάλογα με τους προορισμούς, να αποφύγουν το single point failure ή για το traffic load balancing. Κάθε SEG είναι υπεύθυνο για την κυκλοφορία του NDS/IP σύμφωνα με καθορισμένους με σαφήνεια κανόνες που έχουν τα IP security domains. Κατά προστασία της κυκλοφορίας των inter-domain IMS είναι υποχρεωτικό να παρασχεθεί η εμπιστευτικότητα, η ακεραιότητα στοιχείων, και η αυθεντικοποίηση στο NDS/IP. Οι πύλες ασφάλειας ενισχύουν τις πολιτικές ασφάλειας μεταξύ των δικτύων. Η ασφάλεια μπορεί να περιλάβει πολιτικές φιλτραρίσματος(filtering) καθώς επίσης και τη λειτουργία firewall. Τα SEGs είναι αρμόδια για τις ευαίσθητες διαδικασίες ασφάλειας και πρέπει να εξασφαλιστούν και προστατευτούν φυσικά. Το SEG θα παράσχει κανονικά τουλάχιστον μια σήραγγα IPSec πάντα σε ένα όμοιο SEG. Κάθε SEG είναι αρμόδιο για την οργάνωση και τη διατήρηση των ενώσεων ασφάλειας (security associations) IPSec (SAs) με το όμοιο SEGs του. Αυτά τα SAs διαπραγματεύονται χρησιμοποιώντας το πρωτόκολλο Internet Key Exchange (IKE). Κάθε SEG διατηρεί δύο SAs ανά σύνδεση: ένας για την εισερχόμενη κυκλοφορία και άλλος για την εξερχόμενη κυκλοφορία. Επιπλέον, διατηρεί ένα Internet Security Association και ένα Key Management Protocol (ISAKMP) SA για τη διαχείριση των κλειδιών. Στο NDS/IP, η αυθεντικοποίηση είναι βασισμένη στα λεγόμενα preshared secrets. Το SEG θα διατηρήσει λογικά ένα διαχορισμό του Security Associations Database και του Security Policy Database για κάθε διεπαφή.

Οι λειτουργίες τους δίνονται έως εξής:

- Security Policy Database (SPD). Περιέχει τις πολιτικές από τις οποίες όλη η εισερχόμενη και εξερχόμενη κυκλοφορία ταξινομείται από τις πύλες ασφάλειας(security gateways). Γενικά, τα πακέτα επιλέγονται για το ένα από τους τρεις τρόπους επεξεργασίας που είναι βασισμένοι στις πληροφορίες της επικεφαλίδας(message header) των IP και transport layer που αντιστοιχούνται

με τις καταχωρήσεις στη βάση δεδομένων (SPD). Ένα πακέτο είτε διατεθέτει υπηρεσίες ασφάλειας IPSec, που είτε απορρίπτονται, είτε επιτρέπονται να παρακάμψουν IPSec.

- Security Associations Database (SAD). Είναι ένας container για όλα τα ενεργά SAs, και τις σχετικές παράμετροι. Ένα σύνολο επιλογέων(selectors) χρησιμοποιείται από το SPD για να χαρτογραφήσει την κυκλοφορία σε ένα συγκεκριμένο SA. Αυτή η σχέση αντιπροσωπεύεται από ένα σύνολο πληροφοριών μεταξύ των SEGs. Οι πληροφορίες πρέπει να συμφωνηθούν και να μοιραστούν μεταξύ όλων των SEGs. Κατά την πρόσβαση στα SA στοιχεία, τα SEGs χρησιμοποιούν έναν δείκτη ή ένα προσδιοριστικό που αναφέρεται ως Security Parameter Index (SPI).

2.3 User and Application Domain Security Features

2.3.1 User Domain Security

Η ασφάλεια των περιοχών χρηστών(User domain security) εξασφαλίζει ασφαλή πρόσβαση στα MS. Είναι βασισμένο σε μια φυσική συσκευή αποκαλούμενη κάρτα ολοκληρωμένων κυκλωμάτων UMTS (UMTS Integrated Circuit Card), η οποία μπορεί να εισαχθεί εύκολα και να αφαιρεθεί από τον τερματικό εξοπλισμό, που περιέχει τις εφαρμογές ασφάλειας όπως το USIM. Το USIM αντιπροσωπεύει και προσδιορίζει έναν χρήστη και την ένωσή του με ένα HE. Είναι αρμόδιο για την εκτέλεση της αυθεντικοποίησης των συνδρομητών και των δικτύων, καθώς επίσης και τη συμφωνία για τα κλειδιά, όταν 3G υπηρεσίες ζητούνται. Μπορεί επίσης να περιέχει ένα αντίγραφο των παραμέτρων χρήστη.

Η πρόσβαση στο USIM είναι περιορισμένη σε έναν εξουσιοδοτημένο χρήστη, ή σε διάφορους εξουσιοδοτημένους χρήστες. Για να ολοκληρώσουν αυτό το χαρακτηριστικό γνώρισμα, ο χρήστης και το USIM πρέπει να μοιραστούν ένα μυστικό (π.χ. το PIN). Ο χρήστης παίρνει την πρόσβαση στο USIM μόνο εάν αποδεικνύει τη γνώση του μυστικού. Επιπλέον, η πρόσβαση σε ένα τερματικό ή σε

άλλο εξοπλισμό χρηστών μπορεί να περιοριστεί σε ένα εξουσιοδοτημένο USIM. Για αυτόν τον λόγο, το USIM και το τερματικό πρέπει επίσης να μοιραστούν ένα μυστικό. Εάν ένα USIM αποτυγχάνει να αποδείξει τη γνώση του μυστικού, τότε, η πρόσβαση στο τερματικό δεν επιτρέπεται.

2.3.2 Application Domain Security

Από την άλλη, η ασφάλεια των περιοχών της εφαρμογής(application domain security) εξετάζει την ασφαλή επικοινωνία μεταξύ τουMS και του SN ή του SP πέρα από το δίκτυο με το επίπεδο ασφάλειας που επιλέγεται από το χειριστή δικτύων ή τον προμηθευτή εφαρμογής. Μια remote εφαρμογή πρέπει να αυθεντικοποίηση έναν χρήστη πριν του επιτρέψει να χρησιμοποιήσει τις υπηρεσίες της εφαρμογής, και θα μπορούσε επίσης να επιτρέψει την εμπιστευτικότητα στοιχείων σε επίπεδο εφαρμογής. Οι επιπέδου εφαρμογής μηχανισμοί ασφάλειας απαιτούνται επειδή η λειτουργία των χαμηλότερων στρωμάτων δεν μπορεί να εγγυηθεί την end-to-end παροχή ασφάλειας. Η έλλειψη end-to-end ασφάλειας θα μπορούσε να προβλεφθεί όταν, παραδείγματος χάριν, το μακρινό συμβαλλόμενο μέρος είναι προσιτό μέσω του Διαδικτύου.

Το USIM Application Toolkit παρέχει την ικανότητα για τους χειριστές ή τους προμηθευτές τους(third party providers) να δημιουργήσουν εφαρμογές που θα μπουν στο USIM. Για να βεβαιώσουν τις ασφαλείς συναλλαγές μεταξύ του MS και του SN ή του SP, διάφοροι βασικοί μηχανισμοί ασφάλειας όπως η επικύρωση των οντοτήτων, αυθεντικοποίηση μηνυμάτων, replay detection, ακεραιότητα ακολουθίας (sequence integrity), διαβεβαίωση εμπιστευτικότητας, και η απόδειξη της παραλαβής, έχει διευκρινιστεί και έχει ενσωματωθεί στο USIM Application Toolkit.

Το Wireless Application Protocol (WAP) είναι μια ομάδα προτύπων για την παράδοση και παρουσίαση των υπηρεσιών Διαδικτύου στα ασύρματα τερματικά, που λαμβάνουν υπόψη το περιορισμένο εύρος ζώνης των κινητών δικτύων, καθώς επίσης και τις περιορισμένες ικανότητες επεξεργασίας των κινητών συσκευών. Για να συνδέσει την ασύρματη περιοχή (wireless domain) με το Διαδίκτυο, μια πύλη WAP απαιτείται για να μεταφράσει τα πρωτόκολλα που χρησιμοποιούνται στο τμήματα

WAP στα πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο. Η αρχιτεκτονική WAP έχει τυποποιηθεί σε δύο εκδόσεις (εκδόσεις 1.2.1 και 2.0).

Για να εξασφαλίστει τη μετάδοση των δεδομένων στην αρχιτεκτονική WAP (έκδοση 1.2.1), το Wireless Transport Layer Security πρωτόκολλο (WTLS), που είναι βασισμένο στο πρωτόκολλο TLS, υιοθετείται. Το WTLS έχει βελτιστοποιηθεί για τη χρήση πέρα από τα περιορισμένης ζώνης κανάλια επικοινωνίας που παρέχουν επίσης την υποστήριξη για datagram δεδομένα. Εξασφαλίζει την ακεραιότητα στοιχείων, τη μυστικότητα, την αυθεντικοποίηση, και την προστασία από denial-of-service. Για τις εφαρμογές Ιστού που υιοθετούν τις τυποποιημένες τεχνικές ασφάλειας Διαδικτύου με TLS, η πύλη WAP αυτόματα και διαφανώς διαχειρίζεται την ασύρματη ασφάλεια, και μεταβιβάζει τα προστατευμένα στοιχεία μεταξύ των καναλιών WTLS και TLS. Κατά συνέπεια, αυτό το σχέδιο δεν υποστηρίζει την end-to-end ασφάλεια.

Το WAP 2,0 προχωρά στον επανασχεδιασμό της αρχιτεκτονικής WAP με την εισαγωγή της υπάρχουσας λίστας πρωτοκόλλου Διαδικτύου, συμπεριλαμβανομένου του πρωτοκόλλου Transmission Control Protocol (TCP), στο περιβάλλον WAP. Η νέα αρχιτεκτονική επιτρέπει μια σειρά διαφορετικών gateways, η οποία επιτρέπει τη μετατροπή μεταξύ των δύο protocol stacks οπουδήποτε από την κορυφή στο κατώτατο σημείο του stack. Μια TCP gateway επιτρέπει δύο εκδόσεις του TCP, μια για συνδεμένη με καλώδιο και άλλη για το ασύρματο δίκτυο, πάνω από το οποίο ένα ασφαλές κανάλι TLS μπορεί να καθιερωθεί από την κινητή συσκευή έως τον κεντρικό υπολογιστή. Η διαθεσιμότητα ενός ασύρματου profile του πρωτοκόλλου TLS, που περιλαμβάνει cipher suites, πιστοποιητικά(certificate formats), αλγορίθμους υπογραφής (signing algorithms), και χρήση της συνόδου, επιτρέπουν την end-to-end υποστήριξη ασφάλειας στο επίπεδο μεταφορών που επιτρέπει τη διαλειτουργικότητα για τις ασφαλείς συναλλαγές.

2.3.3 Security Visibility and Configurability

Αν και τα μέτρα ασφάλειας που παρέχονται από το SN πρέπει να είναι διαφανή στον τελικό χρήστη, διαφάνεια των διαδικασιών ασφάλειας τόσο καλά όπως τα υποστηριγμένα χαρακτηριστικά γνωρίσματα ασφάλειας πρέπει να παρασχεθούν.

Αυτό μπορεί να περιλάβει:

- ένδειξη της κρυπτογράφησης δικτύων πρόσβασης (access network encryption)
- ένδειξη της ευρείας κρυπτογράφησης δικτύων (network wide encryption)
- ένδειξη του επιπέδου ασφάλειας (π.χ. όταν κινείται ένας χρήστης από 3G προς 2G).

Η διαμόρφωση (configurability) επιτρέπει στον κινητό χρήστη και στο HE να διαμορφώσει εάν μια παροχή υπηρεσιών πρέπει να εξαρτηθεί από την ενεργοποίηση ορισμένων χαρακτηριστικών γνωρισμάτων ασφάλειας. Μια υπηρεσία μπορεί μόνο να χρησιμοποιηθεί όταν είναι όλα τα σχετικά χαρακτηριστικά γνωρίσματα ασφάλειας σε λειτουργία. Τα διαμορφώσιμα χαρακτηριστικά γνωρίσματα που προτείνονται περιλαμβάνουν:

- επιτρέποντας/απορρίπτοντας αυθεντικοποίηση χρήστη- USIM για ορισμένες υπηρεσίες
- αποδοχή/απόρριψη των εισερχόμενων μη-κρυπτογραφημένων κλήσεων
- οργάνωση ή μη οργάνωση των μη- κρυπτογραφημένων κλήσεων
- αποδοχή/απόρριψη της χρήσης ορισμένων αλγορίθμων κρυπτογράφησης

ΚΕΦΑΛΑΙΟ 3 :
ΑΛΛΑΓΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ UMTS

3. Αλλαγές Ασφάλειας στο UMTS (από την έκδοση 4 στην 8)

3.1 Κωδικοποίηση του Minimum Security Level και του Usim Application Toolkit

Η αλλαγή αυτή έχει παρουσιαστεί στις προδιαγραφές του UMTS έκδοση 5. Η αλλαγή είναι στο “Technical Specification Group Core Network and Terminals; Security mechanisms for the (U)SIM application toolkit; Stage 2 (23048)”.

3.1.1 Sim και Usim Application Toolkit

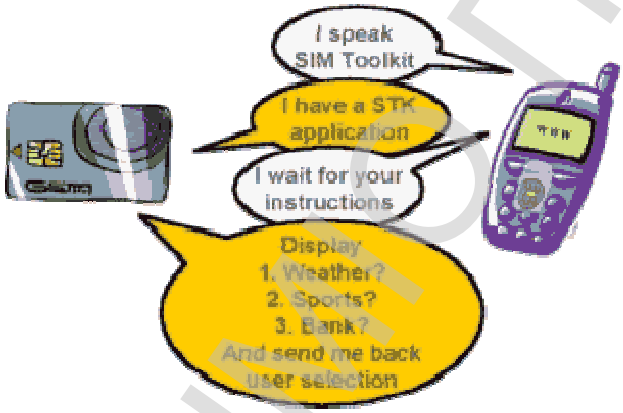
Το SIM Application Toolkit (συνήθως καλούμενο STK) είναι ένα πρότυπο του συστήματος GSM που επιτρέπει στο SIM να αρχίσει τις ενέργειες που μπορούν να χρησιμοποιηθούν για τις διάφορες υπηρεσίες προστιθέμενης αξίας.

Το SIM Application Toolkit αποτελείται από ένα σύνολο εντολών που προγραμματίζονται στην κάρτα SIM και που καθορίζουν πώς το SIM πρέπει να αλληλεπιδράσει άμεσα με τον εξωτερικό κόσμο και αρχίζει τις εντολές ανεξάρτητα από το τηλέφωνο και το δίκτυο. Αυτό επιτρέπει στο SIM να ενισχύσει μια διαλογική ανταλλαγή μεταξύ μιας εφαρμογής δικτύων και του τελικού χρήστη και να έχει πρόσβαση ή να ελέγχει τη πρόσβαση στο δίκτυο. Το SIM δίνει επίσης εντολές στο τηλέφωνο, όπως το display menu και ζητά την εισαγωγή δεδομένων από τους χρήστες.

Το STK έχει επεκταθεί από πολλούς πάροχους κινητής τηλεφωνίας σε όλο τον κόσμο για πολλές εφαρμογές, όπου συχνά μια menu-based προσέγγιση απαιτείται, όπως το Mobile Banking και το σερφάριστα στο Διαδίκτυο. Σχεδιασμένο ως ένα ενιαίο περιβάλλον εφαρμογής, το STK μπορεί να ξεκινήσει με την ενέργεια της κάρτας SIM και ταιριάζει ιδιαίτερα στις χαμηλού επιπέδου εφαρμογές με απλά μενού.

Το USIM Application Toolkit (USAT) είναι το αντίτιμο του STK για τα 3G δίκτυα. Το USAT επιτρέπει στο USIM να αρχίσει τις ενέργειες που μπορούν να χρησιμοποιηθούν για τις διάφορες υπηρεσίες προστιθέμενης αξίας που παραδίδονται στις κινητές συσκευές.

Το USAT εκμεταλλεύεται την πλατφόρμα εφαρμογών 3G των συσκευών με την μη ενεργοποίηση του έως ότου έχει επιλεχτεί μια συγκεκριμένη εφαρμογή, αντίθετα από το STK που ενεργοποιείται στο ξεκίνημα. Μερικές λειτουργίες είναι σχετικές με την κάρτα παρά με την εφαρμογή.



Το SAT/USAT παρέχει τους μηχανισμούς που επιτρέπουν τις εφαρμογές που αποθηκεύονται στο USIM/SIM για να αλληλεπιδράσουν και να λειτουργήσουν με το ME που υποστηρίζουν αυτούς τους μηχανισμούς. Το SAT/USAT παρέχει επίσης έναν μηχανισμό μεταφορών για να κάνει download και να ενημερώσει τις εφαρμογές. Ένα πολύτιμο χαρακτηριστικό γνώρισμα SAT/USAT είναι ότι η κάρτα USIM/SIM προσφέρει ένα ιδιαίτερα ασφαλές περιβάλλον. Ο συνδρομητής, ο εκδότης της κάρτας USIM/SIM και οι εφαρμογές SAT/USAT έχουν μια εμπιστευμένη σχέση που επιτρέπει τα χαρακτηριστικά γνωρίσματα όπως ο έλεγχος κλήσης. Το SAT/USAT API επιτρέπει στους προγραμματιστές της εφαρμογής μια πρόσβαση στις SAT/USAT λειτουργίες και δεδομένα. Χρησιμοποιώντας αυτό το API, οι USIM/SIM υπηρεσίες μπορεί να αναπτυχθούν και να φορτωθούν επάνω στη USIM/SIM αφότου έχει εκδοθεί η κάρτα. Ο μηχανισμός SAT/USAT Mechanisms Profile Download χρησιμοποιείται από το τερματικό για να ενημερώσει το SIM για τις ικανότητες του τερματικού. Το Profile κατεβάζει τις οδηγίες που στέλνονται από το ME στο SIM ως

τμήμα της διαδικασίας έναρξης της SIM. Από αυτήν την διαδικασία το SIM ξέρει τι είμαι ικανός, και το SIM μπορεί έπειτα να περιορίσει τη σειρά εντολών του αναλόγως.

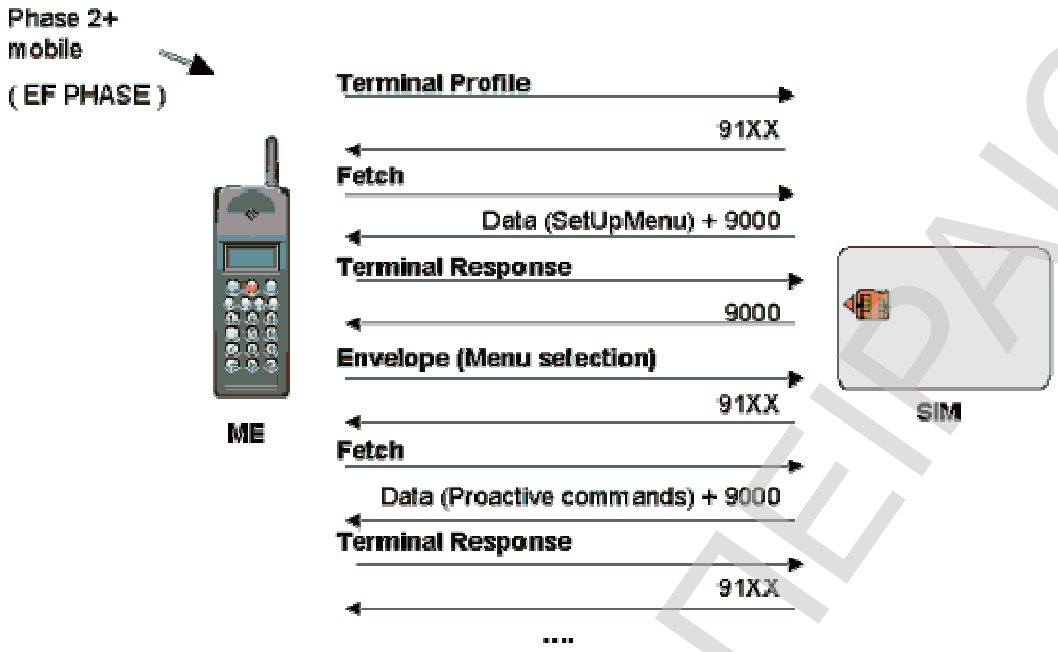
Το δυναμικό (proactive) SIM παρέχει το μηχανισμό για το SIM για να αρχίσει τις ενέργειες που λαμβάνονται από το ME. Από αυτόν τον μηχανισμό η USIM/SIM μπορεί να καθιερώσει και να διατηρήσει έναν interactive διάλογο με το χρήστη και να επικοινωνήσει με το δίκτυο ή μια εξωτερική συσκευή.

Οι δυναμικές (proactive) ενέργειες περιλαμβάνουν:

- επιδεικνύοντας το κείμενο από το SIM στο ME
- αποστολή ενός σύντομου μηνύματος
- οργανώνοντας μια φωνητική κλήση σε έναν αριθμό που έχει το SIM
- καθιέρωση μιας επικοινωνίας με έναν αριθμού ή με το φορέα(bearer) που κατέχει το SIM
- στέλνοντας έναν έλεγχο SS ή ένα USSD string
- παίξιμο του τόνου στο ακουστικό
- έναρξη ενός διαλόγου με το χρήστη
- αίτημα έναρξης του SIM
- παρέχοντας τοπικές πληροφορίες από το ME στο SIM
- επικοινωνία με πρόσθετες κάρτες
- παροχή πληροφοριών για πρόσθετες κάρτες
- διαχείριση των timers που τρέχουν φυσικά στο ME
- τρέξιμο μιας AT εντολής που λαμβάνετε από το SIM, και επιστροφή του αποτελέσματος στο SIM στέλνοντας DTMF
- αίτηση στο ME για να προωθήσει τον browser που αντιστοιχεί σε ένα URL.
- καθιέρωση και διαχείριση ενός ανεξάρτητου πρωτοκόλλου φορέων (bearer independent protocol)

Το ME λέει στο SIM εάν η εντολή ήταν επιτυχής χρησιμοποιώντας τη διαδικασία αποτελέσματος εντολής. Τα αποτελέσματα ομαδοποιούνται σε τρεις κύριους τύπους: ok, προσωρινό πρόβλημα και μόνιμο πρόβλημα. Το download των δεδομένων στο SIM κάνει χρήση μηχανισμών point-to-point SMS ή cell broadcast ή το ανεξάρτητο

πρωτόκολλο φορέων για το download των δεδομένων στο SIM. Ο μηχανισμός επιλογής του menu χρησιμοποιείται για να μεταφέρει την επιλογή της εφαρμογής SIM που επιλέγεται από το χρήστη. Αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί επίσης για την αίτηση των πληροφοριών βοήθειας. Ο έλεγχος κλήσης από το μηχανισμό του SIM επιτρέπει στο SIM να ελέγξει τα dialled strings, τα συμπληρωματικού ελέγχου υπηρεσιών strings και τα USSD strings. Αυτά τα strings περνούν πρώτα στο SIM πριν το ΜΕ οργανώσει μια κλήση, μια συμπληρωματική λειτουργία υπηρεσιών ή τη λειτουργία USSD. Το SIM μπορεί να επιτρέψει, φράξει ή να τροποποιήσει την κλήση. Το SIM μπορεί επίσης να αντικαταστήσει ένα αίτημα κλήσης από ένα άλλο αίτημα κλήσης. Το SIM μπορεί επίσης να επιτρέψει την αποστολή, να φράξει την αποστολή ή να τροποποιήσει τη διεύθυνση προορισμού του σύντομου μηνύματος πριν το στείλει. Ένας download μηχανισμός χρησιμοποιείται για να μεταφέρει τις λεπτομέρειες του γεγονότος στο SIM, όταν εμφανίζεται. Τα γεγονότα (events) περιλαμβάνουν την θέση των εισερχόμενων κλήσεων, και τη διαθεσιμότητα της οθόνης για τις εφαρμογές. Η ασφάλεια μπορεί να απαιτηθεί από τις εφαρμογές για να εξασφαλιστεί η εμπιστευτικότητα στοιχείων, η ακεραιότητα στοιχείων, και η επικύρωση αποστολέων στοιχείων. Πολλαπλάσιοι μηχανισμοί καρτών χρησιμοποιούνται για να ειδοποιήσουν το SIM σε γεγονότα από άλλες κάρτες SIM. Αυτό μπορεί να χρησιμοποιηθεί μόνο όταν υποστηρίζει το τερματικό πολλαπλάσιες κάρτες SIM. Ο μηχανισμός λήξης χρονομέτρων χρησιμοποιείται για να ενημερώσει το SIM πότε ένα χρονόμετρο που τρέχει φυσικά στο ΜΕ λήγει.



3.1.2 Κωδικοποίηση του Minimum Security Level

Το Minimum Security Level (MSL) χρησιμοποιείται για να διευκρινίσει το κατώτατο επίπεδο ασφάλειας που εφαρμόζεται στα εξασφαλισμένα πακέτα (Secured Packets) που στέλνονται στην εφαρμογή. Η λαμβάνουσα οντότητα θα ελέγξει το κατώτατο επίπεδο ασφάλειας πριν επεξεργάζεται την ασφάλεια του πακέτου εντολής (Command Packet). Εάν ο έλεγχος αποτύχει, η λαμβάνουσα οντότητα θα απορρίψει τα μηνύματα και ένα πακέτο απάντησης με "Insufficient Security Level" Response Status Code θα σταλεί αν είναι απαραίτητο.

Εάν το μήκος του Minimum Security Level πεδίου είναι μηδέν, κανένας ελάχιστος έλεγχος επιπέδων ασφάλειας δεν θα εκτελεστεί από τη λαμβάνουσα οντότητα. Εάν το μήκος του Minimum Security Level πεδίου είναι μεγαλύτερο από μηδέν, το Minimum Security Level πεδίο θα κωδικοποιηθεί σύμφωνα με τον ακόλουθο πίνακα:

Length	Name
1	MSL Parameter
q-1	MSL Data

MSL παράμετροι

Value	Name	Support	MSL Data length
'00'	RFU	RFU	N/A
'01'	Minimum SPI1	Optional	1
'02' to '7F'	RFU	RFU	N/A
'80' to 'FE'	Reserved for Proprietary Mechanisms	Optional	N/A
'FF'	RFU	RFU	N/A

Τα Minimum Security Level δεδομένα για την Minimum SPI1 MSL παράμετρο θα χρησιμοποιήσουν την ίδια κωδικοποίηση όπως με το πρώτο octet του SPI ενός πακέτου εντολής.

3.2 Ασφαλής Δομή Πακέτων για τις (U)SIM Toolkit Εφαρμογές

Η αλλαγή αυτή έχει παρουσιαστεί στις προδιαγραφές του UMTS έκδοση 7. Η αλλαγή υπάρχει στο “Technical Specification Group Core Network and Terminals; Secured packet structure for (U)SIM Toolkit applications (31115)”.

3.2.1 Σχετικά με το Unstructured Supplementary Service Data (USSD)

Το USSD (Unstructured Service Supplementary Data) είναι μια τεχνολογία GSM αρχικά προοριζόμενη για χρήση όπου το τηλέφωνο έπρεπε να έχει πρόσβαση στις συμπληρωματικές υπηρεσίες όπως η προώθηση κλήσης και οι multiparty κλήσεις χωρίς επέμβαση από το συνδρομητή. Είναι μια ικανότητα που χτίζεται στα πρότυπα GSM για την υποστήριξη της διαβίβασης των πληροφοριών πέρα από τα κανάλια του δικτύου GSM. Το USSD παρέχει το session-based στην επικοινωνία, επιτρέποντας ποικίλες εφαρμογές.

Ο φορέας(bearer) USSD προσεγγίζεται με την κλήση ενός αριθμού που αρχίζει με τους χαρακτήρες αστερίσκου ή τους hash χαρακτήρες "*" ή "#" και έπειτα έναν συνδυασμό αριθμών, αστερίσκων και τελικά το χαρακτήρα "#". Το τηλέφωνο αναγνωρίζει τέτοιους αριθμούς και θα χρησιμοποιήσει το φορέα USSD αντί μιας

κλήσης φωνής. Αντί της κλήσης ενός άλλου συνδρομητή ή μιας υπηρεσίας, το τηλέφωνο επικοινωνεί με την υποδομή USSD.

Οι πρώτες υπηρεσίες USSD ονομάστηκαν Phase, ή MAP και ήταν μόνο ικανές να περάσουν τις πληροφορίες από το τηλέφωνο στην εφαρμογή USSD με μια επιβεβαίωση. Δεν υπήρξε επομένως καμία σύνοδος που έγινε μεταξύ του τηλέφωνο και της εφαρμογής. Το Phase 2 (ή MAP 2) USSD πρόσθεσε την ικανότητα για να καθιερώσει μια σύνοδο αντί μιας απλής συναλλαγής. Αυτό σήμανε ότι το τηλέφωνο και η εφαρμογή USSD θα μπορούσαν τώρα να έχουν το τεχνικό ανάλογο ενός διαλόγου. Τα τηλέφωνο GSM υποστήριξαν το USSD από τις πρώτες ημέρες του GSM, έτσι αντίθετα από το SMS, κάθε τηλέφωνο GSM υποστηρίζει το USSD. Η Phase 2 έχει υποστηριχθεί για χρόνια και πάνω από 99% των τηλεφώνων αυτήν την περίοδο έχει σε χρήση και μπορεί να χρησιμοποιήσει τις συνόδους ενός φορέα USSD.

Τα περισσότερα τηλέφωνα υποστηρίζουν επίσης το NI USSD (network initiated USSD), αποκαλούμενο επίσης USSD Push. Με το NI USSD, το δίκτυο μπορεί να ωθήσει τις πληροφορίες στο τηλέφωνο του συνδρομητή.

Ένα άλλο σημαντικό γεγονός για το USSD, είναι ότι τα μηνύματα από τα τηλέφωνα πάνε πάντα στο εγχώριο δίκτυο(home network). Αυτό σημαίνει ότι εάν κάνουμε roaming σε ένα άλλο δίκτυο, κατόπιν ο σχηματισμός ενός USSD string στο τηλέφωνό σας θα καθοδηγήσει πάντα στην εφαρμογή στο εγχώριο δίκτυό σας. Εάν το χρησιμοποιήσετε στην πρόσβαση μιας ιδιαίτερης υπηρεσίας στο εγχώριο δίκτυό σας, κατόπιν θα είστε σε θέση επίσης να έχετε πρόσβαση από μια άλλη χώρα. Αντιθέτως, οι συνδρομητές roaming από άλλα δίκτυα δεν μπορούν να έχουν πρόσβαση στις υπηρεσίες USSD σε ένα άλλο host network.

Η διαλογική φύση του USSD επιτρέπει μια εφαρμογή για να δοθούν οι επιλογές συνδρομητών υπό μορφή επιλογών ενός μενού. Αυτές οι επιλογές δεν αποθηκεύονται στο τηλέφωνο και έχουν πραγματικά πολύ λίγα που κάνουν με το USSD. Το USSD δεν είναι ένα μενού στο τηλέφωνο όπως θεωρείται συχνά, αλλά ο φορέας για το μενού. Τα μενού είναι επίσης ανεξάρτητα από το τηλέφωνο καθώς επίσης και την κάρτα SIM. Είναι στη server-side εφαρμογή για να παρακολουθήσει όπου στο μενού επιλογών κάθε συνδρομητής είναι όλη την ώρα.

Ο συνδρομητής δεν είναι απαραίτητο να πάρει το ειδικό λογισμικό για το τηλέφωνο ή τις ειδικές κάρτες SIM για να είναι σε θέση να έχει πρόσβαση στο USSD. Αυτό ασκεί τεράστια επίδραση στη λήψη των υπηρεσιών και οι πάροχοι των δικτύων GSM αναγνωρίζουν τώρα αυτό το όφελος.

Τα μενού που εξυπηρετούνται από το USSD δεν πρέπει να τα συγχέουμε με τα μενού και τις εφαρμογές που εξυπηρετούνται από το STK (Sim Tool Kit). Το STK είναι μια τεχνολογία που ενσωματώνεται στην κάρτα SIM όπου οι ειδικές εφαρμογές μπορούν να προσεγγιστούν από το συνδρομητή. Με το STK, το τηλέφωνο λαμβάνει τις οδηγίες από την κάρτα SIM για να εκτελέσει τις λειτουργίες. Μια δημοφιλής εφαρμογή είναι το WIB (wireless Internet browser). Το WIB γίνετε download επάνω στην κάρτα SIM πριν από τη διανομή και εμφανίζεται στα τηλεφωνικά μενού του συνδρομητή ως σειρά των υπηρεσιών. Το WIB επικοινωνεί με έναν κεντρικό υπολογιστή στο δίκτυο του πάροχου των δικτύων GSM που τον συνδέει με άλλους κεντρικούς υπολογιστές που προσφέρουν τις υπηρεσίες. Ο φορέας(bearer) επικοινωνίας που χρησιμοποιείτε συνήθως είναι το SMS. Το αποτέλεσμα είναι ότι τέτοιες υπηρεσίες είναι πολύ αργές και τις περισσότερες φορές ενοχλητικές. Συνήθως, STK θα χρησιμοποιήσει το SMS ως φορέα για την επικοινωνία.

Το STK ως τεχνολογία μπορεί να χρησιμοποιήσει το USSD ως φορέα, αλλά εξαρτάται πολύ από την εφαρμογή STK σε κάθε τηλέφωνο. Μερικοί κατασκευαστές τηλεφώνων δεν εφάρμοσαν επαρκώς την υποστήριξη STK για το USSD. Το αποτέλεσμα είναι ότι στην πράξη, το STK θα χρησιμοποιήσει πάντα μόνο SMS ως φορέα.

Το USSD διαφέρει από τον άλλο φορέα μηνυμάτων, το SMS, με διάφορους σημαντικούς τρόπους. Δεν είναι store-and-forward φορέας όπως το SMS, αλλά ένας διαφανές session-based φορέας για την πραγματοποιήσει συναλλαγών. Οι πληροφορίες παραδίδονται και οι απαντήσεις αποκτώνται σε πραγματικό χρόνο. Με απλά λόγια, το USSD είναι παρόμοιο με την ομιλία με κάποιον σε ένα τηλέφωνο και το SMS σαν να στέλνει μια επιστολή. Το USSD δεν είναι επίσης ένας point-to-point φορέας όπως το SMS. Ένας συνδρομητής δεν μπορεί να στείλει ένα άλλο κείμενο χρησιμοποιώντας το USSD εκτός αν υπάρχει μια ειδική εφαρμογή στο δίκτυο που να

προσφέρει μια τέτοια δυνατότητα. Κάποιος μπορεί να στείλει 182 χαρακτήρες χρησιμοποιώντας το USSD, αλλά το SMS επιτρέπει μόνο 140 x 8-bit, ή 160 x 7-bit χαρακτήρες. Όπως το SMS, το USSD χρησιμοποιεί τα κανάλια ελέγχου του GSM για τη μεταφορά δεδομένων. Το SMS και το USSD χρησιμοποιούν το SDCCH (αυτόνομο stand-alone dedicated control channel) όταν δεν είναι το τηλέφωνο σε μια κλήση. Όταν το τηλέφωνο είναι πολυάσχολο με μια κλήση, το USSD θα χρησιμοποιήσει το FACCH (fast associated control channel) με μια σημαντική βελτίωση στην ταχύτητα μεταφοράς (1000 bits/second). Αυτή η χρήση του καναλιού SDCCH οδηγεί σε ένα μειονέκτημα με USSD.

Επειδή το κανάλι SDCCH χρησιμοποιείται επίσης από το GSM για την οργάνωση της κλήσης, πολλές ανοικτές σύνοδοι USSD μπορούν να περιορίσουν τις νέες οργανώσεις κλήσεων σε συμφωρισμένα δίκτυα. Στην πράξη, αυτό δεν συμβαίνει συχνά και οι πάροχοι του δικτύου GSM μπορούν να αναβαθμίσουν τους ασύρματους πόρους στα ιδιαίτερα συμφωρισμένα κελιά (congested cells) για να αποτρέψει αυτό από να συμβεί. Αντίθετα από τα SMS, ο συνδρομητής δεν είναι απαραίτητο να δημιουργήσει ένα μήνυμα. Το USSD string μπορεί ακόμη και να αποθηκευτεί στον τηλεφωνικό κατάλογο με ένα όνομα. Μερικές εφαρμογές θα επιτρέψουν επίσης τη δημιουργία menu shortcuts όταν ο συνδρομητής επιλέγει το "*" χαρακτήρα. Στο προηγούμενο παράδειγμά μας, ο χρήστης μπορεί να δημιουργήσει μια εγγραφή "Καιρός Αθήνα" με τον αριθμό * 150*1234*12*3 #. Τα πρόσθετα "* 3" δείχνουν την επιλογή στο menu του 3. Σε ένα επίπεδο δικτύων GSM, η πύλη USSD ορίζεται ως ένα gsmSCF (GSM Service Control Function), ενώ το SMSC ορίζεται ως ένα άλλο HLR (Home Location Register).

Για να συνοψίσουμε, το USSD καθορίζεται μέσα από τα πρότυπα του GSM στα έγγραφα GSM 02.90 (USSD Stage 1) και GSM 03.90 (USSD Stage 2).

Οι βασικές ιδιότητες είναι:

- Το USSD είναι session oriented, αντίθετα με το SMS, το οποίο είναι store-and-forward και transaction-oriented τεχνολογία

- Οι χρόνοι απόκρισης για τις interactive εφαρμογές είναι πιό σύντομοι για το USSD από το SMS λόγω του session-based χαρακτηριστικού γνωρίσματος του USSD, και επειδή δεν είναι store and forward service υπηρεσία.
- Οι χρήστες δεν χρειάζεται να έχουν πρόσβαση σε οποιεσδήποτε ιδιαίτερες τηλεφωνικές επιλογές στις υπηρεσίες πρόσβασης με το USSD - μπορούν να εισαγάγουν τη Unstructured Supplementary Services Data (USSD) εντολή άμεσα από την αρχική οθόνη του κινητού τηλεφώνου.
- Οι εντολές USSD καθοδηγούνται πίσω στον Home Location Register του home δικτύου, επιτρέποντας την δημιουργία ενός virtual home περιβάλλοντος - η δυνατότητα για τις υπηρεσίες (που βασίζονται στο USSD σε αυτήν την περίπτωση) εργάζονται εξ ίσου καλά και με ακριβώς τον ίδιο τρόπο όταν κάνουν roaming οι χρήστες
- Το Unstructured Supplementary Services Data (USSD) λειτουργεί σε όλα τα υπάρχοντα κινητά τηλέφωνα GSM.
- Και το SIM Application Toolkit και το ασύρματο πρωτόκολλο εφαρμογής υποστηρίζει το USSD.

Η Orange Mobile υποστηρίζει αυτό το πρωτόκολλο με την υπηρεσία Orange Money. Το Orange Money προσφέρει έναν απλό, ασφαλή, και αποδοτικό τρόπο στο να λύσει προβλήματα με το να αφήσουν σε σας να κάνετε τις βασικές τραπεζικές εργασίες σας άμεσα στο κινητό τηλέφωνό σας, ένα όφελος για πολλούς ανθρώπους στις αναδυόμενες χώρες. Μόλις γραφτείτε στην υπηρεσία, η οποία είναι συμβατή με όλες τις κινητές συσκευές, έχετε αυτόματη πρόσβαση σε όλα τα χαρακτηριστικά γνωρίσματα του μενού. Μπορείτε να χρησιμοποιήσετε τις κινητές τηλεφωνικές διεπαφές (USSD [Unstructured Supplementary Service Data] μενού, SMS) για να πραγματοποιήσετε τη συναλλαγή σας και να λάβετε την επιβεβαίωση από την από το άλλο συμβαλλόμενο μέρος, που διευκολύνει το μυαλό σας για εάν τα χρήματα έχουν παραληφθεί. Μπορείτε επίσης να ελέγξετε τελευταίες πέντε συναλλαγές σας στον κινητό.

3.2.2 Εφαρμογή του USSD

Ο τρόπος εφαρμογής του USSD επιτρέπει τη διάφανη μεταφορά των δεδομένων μεταξύ μιας εφαρμογής που κατοικεί στο δίκτυο και μιας βασισμένης στο UICC εφαρμογής. Σε αυτή την περίπτωση, για να εξασφαλίσουν το ωφέλιμο φορτίο (payload) των διαδικασιών USSD, οι μηχανισμοί ασφάλειας καθορίζονται και θα εφαρμοστούν στα μηνύματα USSD. Το Generic secured Command Packet και το secured Response Packet περιλαμβάνονται στο UM του USSD String.

3.2.2.1 Δομή των Ασφαλών Πακέτων Εντολών (Secure Command Packet) που Υπάρχουν σε ένα Μονό USSD Μήνυμα

Το πεδίο UM ενός USSD String περιέχει το Command Packet. Το Command Packet θα κωδικοποιηθεί ως ένα γενικό Command Packet. Στο Command Packet, η τιμή του Command Packet Identifier (CPI) είναι 03 και το Command Header Identifier (CHI) είναι κενή τιμή. Τα CPI, CPL και CHL θα περιληφθούν στον υπολογισμό του RC/CC/DS.

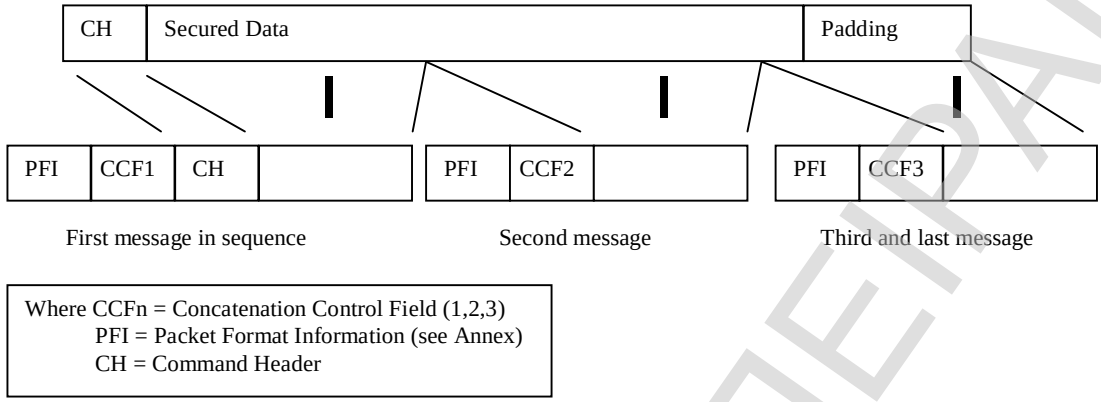
3.2.2.2 Δομή των Πακέτων Εντολών (Command Packet) που Υπάρχουν σε ένα Ενωμένο USSD Μήνυμα

Εάν το Command Packet είναι μακρύτερο από 159 bytes (συμπεριλαμβανομένου του Command Header) έπειτα θα αντιμετωπιστεί ως εξής.

- Όλο το Command Packet συμπεριλαμβανομένου του Command Header θα χωριστεί στα συστατικά του μέρη (component concatenated parts).
- Το Command Packet αντιμετωπίζεται ως συνδεδεμένο USSD.
- Το Command Packet Header θα είναι μόνο παρών στο πρώτο τμήμα ενός συνδεδεμένου μηνύματος (concatenated message).

Εάν τα δεδομένα κρυπτογραφούνται, τότε κρυπτογραφούνται όπως περιγράφεται ανωτέρω, πρίν χωριστούν σε μεμονωμένα συνδεδεμένα δεδομένα. Τα CPI, CPL και CHL θα περιληφθούν στον υπολογισμό του RC/CC/DS. Ένα παράδειγμα που

επεξηγεί ένα Command Packet που χωρίζεται πέρα από μια ακολουθία τριών μηνυμάτων παρουσιάζεται κατωτέρω.



Example of command split using concatenated USSD messages

3.2.2.3 Δομή του Πακέτου Απάντησης (Response Packet)

Το πακέτο απάντησης(Response Packet) παράγεται από τη λαμβάνουσα οντότητα (Receiving Entity) και περιλαμβάνει ενδεχομένως μερικά στοιχεία που παρέχονται από τη λαμβάνουσα εφαρμογή, και που επιστρέφονται στην οντότητα αποστολής/εφαρμογή αποστολής της αίτησης. Στην περίπτωση όπου η λαμβάνουσα οντότητα είναι το UICC, αυτό το πακέτο απάντησης παράγεται στο UICC, ανακτάται από το ME από το UICC, και περιλαμβάνεται στο τμήμα επιστροφής αποτελέσματος ενός Facility μηνύματος που επιστρέφεται στο δίκτυο.

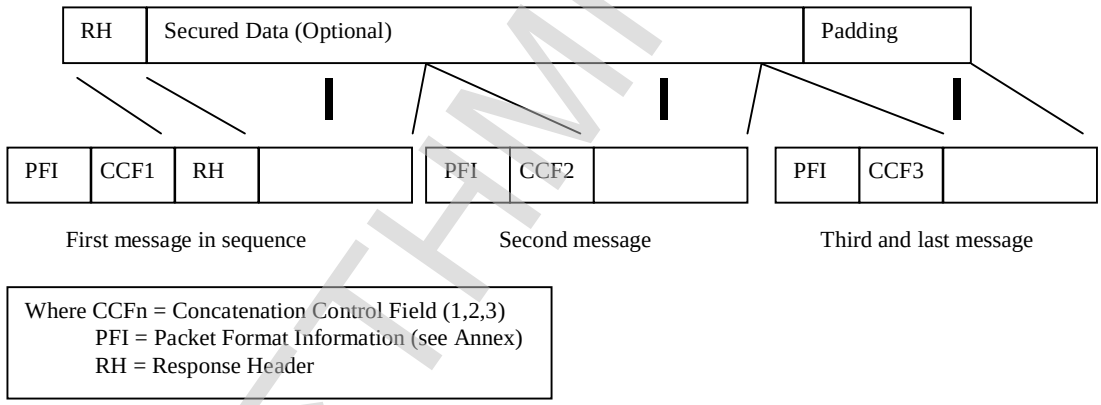
Στο πακέτο απάντησης (Response Packet), το Response Packet Identifier (RPI) είναι 04 και το Response Header Identifier(RHI) είναι μια κενή τιμή. Τα RPI, RPL και RHL θα περιληφθούν στον υπολογισμό του RC/CC/DS.

3.2.2.4 Structure of the Response Packet contained in concatenated USSD Messages

Εάν το Response Packet είναι μακρύτερο από 159 bytes (συμπεριλαμβανομένου του Response Header) έπειτα θα αντιμετωπιστεί ως εξής.

- Όλο το Response Packet συμπεριλαμβανομένου του Response Header θα χωριστεί στα συστατικά του μέρη (component concatenated parts).
- Το Response Packet αντιμετωπίζεται ως συνδεδεμένο USSD.
- Το Response Packet Header θα είναι μόνο παρών στο πρώτο τμήμα ενός συνδεδεμένου μηνύματος (concatenated message).

Εάν τα δεδομένα κρυπτογραφούνται, τότε κρυπτογραφούνται όπως περιγράφεται ανωτέρω, πρίν χωρίστούν σε μεμονωμένα συνδεδεμένα δεδομένα. Τα RPI, RPL και RHL θα περιληφθούν στον υπολογισμό του RC/CC/DS. Ένα παράδειγμα που επεξηγεί ένα Response Packet που χωρίζεται πέρα από μια ακολουθία τριών μηνυμάτων παρουσιάζεται κατωτέρω.



Example of Response split using concatenated USSD messages

3.3 Χρήση του TCAP handshake στα SMS

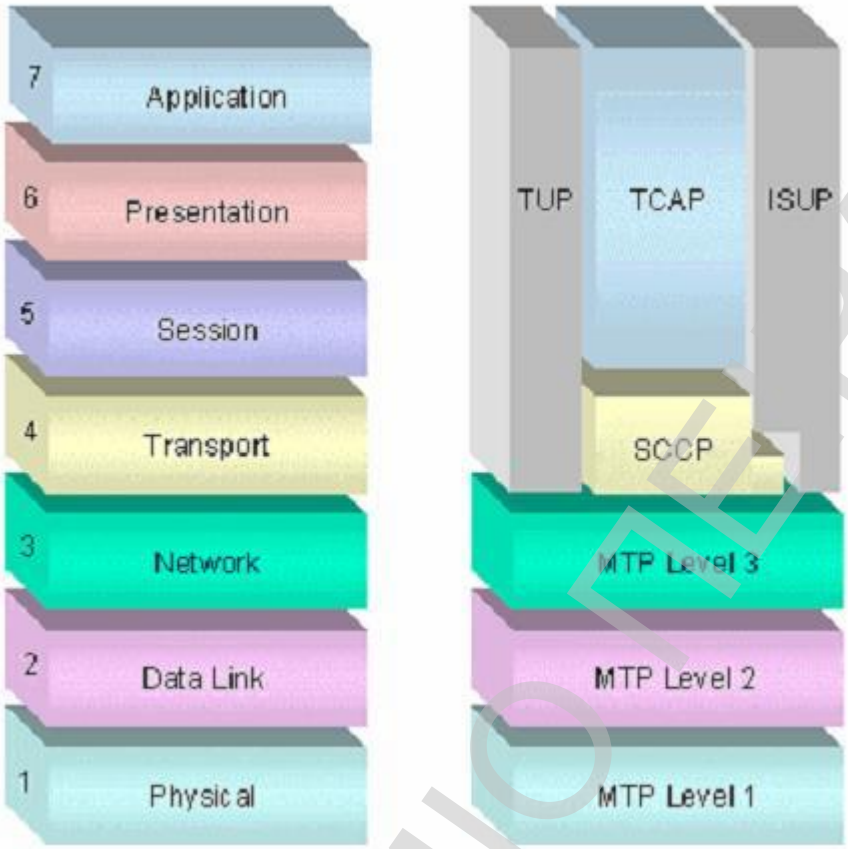
Η αλλαγή αυτή έχει παρουσιαστεί στις προδιαγραφές του UMTS έκδοση 6. Η αλλαγή είναι στο “Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; MAP application layer security (33200)”.

Η χρήση της χειραψίας(handshake) TCAP για τη μεταφορά sms εισάγεται στην έκδοση 6. Ο πάροχος του SMS Gateway/Interworking MSC και ο πάροχος του serving node (MSC or SGSN) μπορούν να συμφωνήσουν να χρησιμοποιήσουν τη χειραψία TCAP ως αντίμετρο ενάντια στην απάτη με τα SMS για τα μηνύματα που ανταλλάσσονται μεταξύ των δικτύων τους. Ένα περιορισμένο επίπεδο αυθεντικοποίησης παρέχεται από τους ακόλουθους μηχανισμούς.

3.3.1 Signaling System #7 (SS7)

Το SS7 είναι η σπονδυλική στήλη των κινητών δικτύων. Είναι το πρωτόκολλο που κάνει την κινητή τηλεφωνία να δουλέψει. Το SS7 είναι το πρωτόκολλο που καθιστά την επικοινωνία μεταξύ των οντοτήτων των δικτύων πιθανή. Η SS7 δομή δικτύων είναι πάρα πολύ παρόμοια με τη δομή δικτύων TCP/IP. Όπως μπορείτε να δείτε από την εικόνα του πρωτόκολλο SS7 που προέρχεται από το πρότυπο OSI και έχει όλα τα 7 διαφορετικά στρώματα.

Στο TCP/IP έχετε την κάρτα Ethernet ως υλικό σας και στο SS7 έχετε τις SS7 κάρτες (signaling cards). Για το TCP/IP έχετε τις διευθύνσεις IP που δίνουν μια λογική δομή στο δίκτυο. Στο SS7 έχετε τους κώδικες σημείου (point codes).



Τα SS7 πρωτόκολλα έχουν αναπτυχθεί από την AT&T από το 1975 και έχουν οριστεί ως τα πρότυπα από το ITU-T κατά τη διάρκεια του 1981 στις συστάσεις του ITU-T's Q.7XX-series. Το SS7 είχε ως σκοπό να αντικαταστήσει το Signaling System #5 (SS5), το Signaling System #6 (SS6) και R2, τα οποία είναι πρότυπα ITU που καθορίζονται από το ITU-T πριν από το SS7 και κάποτε ήταν σε διαδεδομένη διεθνή χρήση. Το SS7 έχει αντικαταστήσει ουσιαστικά τα SS6, SS5 και R2, με εξαίρεση ότι στο R2 οι παραλλαγές χρησιμοποιούνται ακόμα από πολλά έθνη. Το SS5 και τα νωρίτερα πρωτόκολλα χρησιμοπούν in-band signaling, όπου οι πληροφορίες για οργάνωση της κλήσης στάλθηκαν με το παίξιμο των ειδικών πολυσυχνικών τόνων στις τηλεφωνικές γραμμές (γνωστές ως κανάλια φορέων στη γλώσσα της βιομηχανίας τηλεπικοινωνιών). Αυτό οδήγησε στα προβλήματα ασφάλειας με τα μπλε κουτιά. Τα σύγχρονα σχέδια του τηλεφωνικού εξοπλισμού που εφαρμόζουν το out-of-band signaling κρατούν ρητά τον ήχο του τελικού χρήστη, που αποκαλείτε και ομιλία, χωριστά από τη σηματοδότηση ώστε να μειώσει τη πιθανότητα ότι οι τελικοί χρήστες

θα μπορούν να εισαγάγουν τόνους που θα μπερδεύονταν με εκείνους που χρησιμοποιούνται για τη σηματοδότηση.

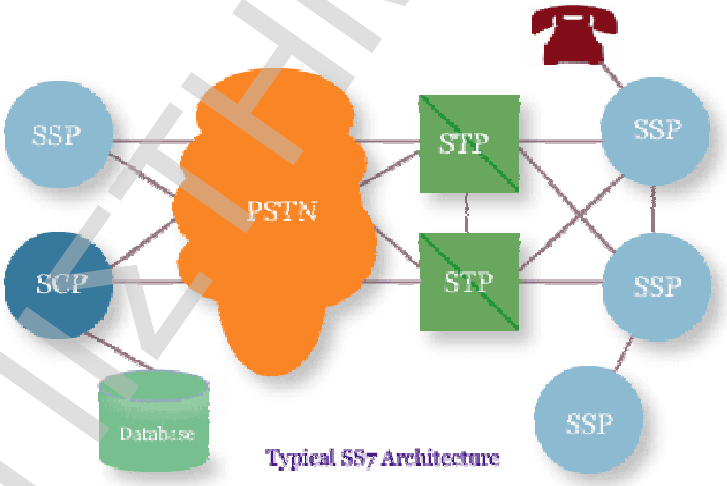
Τα SS6 και SS7 κινηθήκαν προς ένα σύστημα στο οποίο οι πληροφορίες signaling ήταν εκτός ζώνης (out-of-band), σε ένα χωριστό κανάλι σήματος. Αυτό έλυσε τα προβλήματα ασφάλειας που τα προηγούμενα συστήματα είχαν, δεδομένου ότι ο τελικός χρήστης δεν είχε καμία σύνδεση σε αυτά τα κανάλια. Τα SS6 και SS7 αναφέρονται ως Common Channel Interoffice Signaling Systems (CCIS) ή Common Channel Signaling (CCS) που οφείλεται στο σκληρό χωρισμό τους καναλιών σηματοδότησης και φορέων (bearer channels). Εντούτοις απαίτησε επίσης και ένα χωριστό κανάλι που αφιερώθηκε απλώς στη σηματοδότηση, αλλά λόγω της γρήγορης ανόδου στον αριθμό διαθέσιμων καναλιών συγχρόνως αυτό ήταν ένα αμφισβητήσιμο σημείο.

Υπάρχουν δύο ουσιαστικά συστατικά σε όλα τα τηλεφωνήματα. Το πρώτο, και προφανέστερο, είναι οι πραγματικές οι φωνές, τα fax, τα στοιχεία ενός modem κ.λπ. Το δεύτερο είναι οι πληροφορίες που καθοδηγούν τις τηλεφωνικές ανταλλαγές για να εγκαταστήσουν τις συνδέσεις και να καθοδηγήσουν το περιεχόμενο σε έναν κατάλληλο προορισμό. Το τηλεφωνικό σήμα ενδιαφέρεται για τη δημιουργία των προτύπων για τα τελευταία για να επιτύχει τα πρώτα. Αυτά τα πρότυπα είναι γνωστά ως πρωτόκολλα SS7 ή Signaling System Number 7 και είναι απλά ένα άλλο σύνολο πρωτοκόλλων που περιγράφουν έναν τρόπο επικοινωνίας μεταξύ των τηλεφωνικών μεταβάσεων στα δημόσια τηλεφωνικά δίκτυα. Έχουν δημιουργηθεί και έχουν ελεγχθεί από τους διάφορους οργανισμούς σε όλο τον κόσμο, το οποίο οδηγεί σε μερικές συγκεκριμένες τοπικές παραλλαγές, αλλά η κύρια οργάνωση με την ευθύνη για τη διοίκησή τους είναι η International Telecommunications Union ή αλλιώς ITU-T.

Η μέθοδος του signaling στο SS7 χρησιμοποιεί την ίδια φυσική πορεία και για το call-control signaling και η πραγματική συνδεδεμένη κλήση. Αυτή η μέθοδος είναι ανεπαρκής και αντικαθίσταται γρήγορα από τις εκτός ζώνης (out-of-band) ή τις common-channel signaling τεχνικές. Για να καταλάβουμε το SS7 πρέπει πρώτα να καταλάβουμε κάτι από τη βασική ανεπάρκεια των προηγούμενων signaling μεθόδων που χρησιμοποιούνται στο Public Switched Telephone Network (PSTN). Μέχρι

σχετικά πρόσφατα, όλες οι τηλεφωνικές συνδέσεις ρυθμίστηκαν από ποικίλες τεχνικές που τοποθετήθηκαν κεντρικά σε in band signaling.

Τα αρχικά interoffice signaling πρωτόκολλα βασίστηκαν στο Signaling System Number 6 (SS#6). Σήμερα το SS#7 χρησιμοποιείται στις νέες εγκαταστάσεις παγκοσμίως. Το SS#7 είναι το καθορισμένο interoffice signaling πρωτόκολλο για το ISDN. Είναι επίσης σε μεγάλη χρήση σήμερα έξω από το περιβάλλον ISDN. Η κύρια λειτουργία του SS#7 είναι να παρασχεθεί ο έλεγχος κλήσης, η μακρινή διαχείριση των δικτύων, και οι δυνατότητες συντήρησης για το διά - τηλεφωνικό δίκτυο. Το SS#7 εκτελεί αυτές τις λειτουργίες με την ανταλλαγή των μηνυμάτων ελέγχου μεταξύ των SS#7 τηλεφωνικών ανταλλαγών (signaling points ή SPs) και του SS#7 signaling transfer points (STPs). Τα switching offices (SPs) χειρίζονται το SS#7 δίκτυο ελέγχου καθώς επίσης και το circuit-switched δίκτυο χρηστών. Βασικά, το SS#7 δίκτυο ελέγχου λέει στο switching office τις πορείες που υπάρχουν πέρα από το circuit-switched δίκτυο. Τα STP οδηγεί τα SS#7 πακέτα (control packets) μέσω του δικτυού σημάτων. Ένα switching office μπορεί ή δεν να είναι ένα STP.



Typical SS7 Architecture

3.3.2 Mobile Application Part (MAP)

Το Mobile Application Part (MAP) είναι ένα SS7 πρωτόκολλο που παρέχει ένα στρώμα εφαρμογής για τους διάφορους κόμβους στα κινητά κεντρικά δίκτυα GSM

και UMTS και τα κεντρικά GPRS δίκτυα που επικοινωνούν το ένα με το άλλο προκειμένου να παρασχεθούν οι υπηρεσίες στους τηλεφωνικούς χρήστες. Το Mobile Application Part είναι το πρωτόκολλο εφαρμογή-στρώματος(application-layer protocol) που χρησιμοποιείται για να υπάρχει πρόσβαση στα Home Location Register, Visitor Location Register, Mobile Switching Center, Equipment Identity Register, Authentication Centre, Short message service center και Serving GPRS Support Node.

Οι βασικές υπηρεσίες που παρέχει το MAP είναι:

- Υπηρεσίες Mobility: διαχείριση θέσης (όταν κινούνται οι συνδρομητές μέσα ή μεταξύ των δικτύων), αυθεντικοποίηση, πληροφορίες για διαχείριση των υπηρεσιών, αποκατάσταση προβλημάτων,
- Operation and Maintenance: εντοπισμός συνδρομητών, ανάκτηση του IMSI των συνδρομητών
- Call Handling: δρομολόγηση, χειρισμός κλήσεων ενώ γίνετε roaming ελέγχοντας ότι ένας συνδρομητής είναι διαθέσιμος για να λάβει τις κλήσεις
- Συμπληρωματικές υπηρεσίες (Supplementary Services)
- Υπηρεσίες SMS (Short Message Service)
- Packet Data Protocol (PDP) υπηρεσίες για το GPRS: παροχή πληροφοριών για την δρομολόγηση στις GPRS συνδέσεις
- Location Service Management Services: ανάκτηση της τοποθεσίας των συνδρομητών

Το MAP είναι ένας χρήστης Transaction Capabilities Application Part (TCAP), και μπορεί υπό αυτήν τη μορφή να μεταφερθεί χρησιμοποιώντας τα παραδοσιακά SS7 πρωτόκολλα ή πάνω από το IP που χρησιμοποιεί το SIGTRAN μέσω ενός κατάλληλου στρώματος προσαρμογής όπως το SCCP User Adaptation (SUA) ή το MTP3 User Adaptation (M3UA) στρώμα.

3.3.3 Transaction Capabilities Application Part (TCAP)

Το Transaction Capabilities Application Part (TCAP), ένα πρωτόκολλο των SS7 πρωτοκόλλων, επιτρέπει την επέκταση των προηγμένων υπηρεσιών έξυπνων δικτύων με την υποστήριξη της ανταλλαγής non-circuit πληροφοριών μεταξύ των signaling points που χρησιμοποιούν την Signalling Connection Control Part (SCCP) connectionless υπηρεσία. Το TCAP υποστηρίζει επίσης τον τηλεχειρισμό, μια δυνατότητα να κληθούν τα χαρακτηριστικά γνωρίσματα σε ένα άλλο μακρινό network switch. Στα κινητά δίκτυα (IS-41 και GSM), το TCAP μεταφέρνει το Mobile Application Part (MAP) που στέλνονται μεταξύ των mobile switches και των βάσεων δεδομένων στην επικύρωση χρηστών υποστήριξης, τον προσδιορισμό εξοπλισμού, και το roaming.

Το κομμάτι της συναλλαγής TCAP περιέχει ένα package type identifier με τους ακόλουθους τύπους πακέτων:

- Unidirectional: Τα κομμάτι των μεταφορών (transfers component) σε μια κατεύθυνση μόνο (καμία απάντηση αναμενόμενη).
- Query with Permission: Αρχίζει μια συναλλαγή TCAP (π.χ., ένα query 1-800). Ο κόμβος προορισμού μπορεί να τελειώσει τη συναλλαγή.
- Query without Permission: Αρχίζει μια συναλλαγή TCAP. Ο κόμβος προορισμού μπορεί να μην τελειώσει τη συναλλαγή.
- Response: Τελειώνει μια συναλλαγή TCAP. Μια απάντηση σε ένα query 1-800 με άδεια μπορεί να περιέχει τον αριθμό δρομολόγησης που συνδέεται με τον αριθμό 800.
- Conversation with Permission: Συνεχίζει μια συναλλαγή TCAP. Ο κόμβος προορισμού μπορεί να τελειώσει τη συναλλαγή.
- Conversation without Permission: Συνεχίζει μια συναλλαγή TCAP. Ο κόμβος προορισμού μπορεί να μην τελειώσει τη συναλλαγή.
- Abort: Ολοκληρώνει μια συναλλαγή εξαιτίας μιας ανώμαλης κατάστασης.

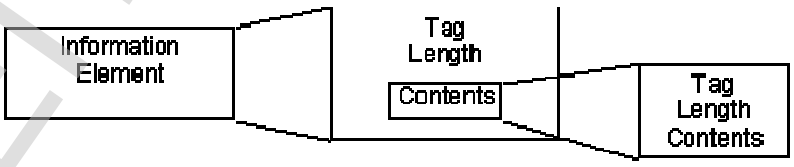
Η μερίδα συναλλαγής περιέχει επίσης το Originating Transaction ID και το Responding Transaction ID πεδίο που συνοδεύει μια συναλλαγή TCAP με μια

συγκεκριμένη εφαρμογή στα σήμα σημεία δημιουργίας και προορισμού των signaling points αντίστοιχα.

Το κομμάτι του TCAP περιέχει συστατικά όπως τα παρακάτω:

- Invoke (Last): Επικαλείται μια λειτουργία. Παραδείγματος χάριν, μια συναλλαγή Query with Permission μπορεί να περιλάβει ένα Invoke (Last) κομμάτι για να ζητήσει την SCP μετάφραση ενός σχηματισμένου αριθμού πχ 800. Το συστατικό αυτό είναι το τελευταίο από τα συστατικά σε ένα query.
- Invoke (Not Last): Παρόμοιο με Invoke (Last) συστατικό εκτός από το ότι αυτό το συστατικό ακολουθείται από ένα ή περισσότερα άλλα συστατικά.
- Return Result (Last): Επιστρέφει το αποτέλεσμα μιας κληθείσας λειτουργίας (invoked operation). Το συστατικό αυτό είναι το τελευταίο από τα συστατικά σε ένα query.
- Returns the result of an invoked operation. Το συστατικό αυτό είναι το τελευταίο από τα συστατικά σε μια απάντηση.
- Return Result (Not Last): Παρόμοιο με το Return Result (Last) κομμάτι αποτελέσματος (εκτός από το ότι το συστατικό αυτό ακολουθείται από ένα ή περισσότερα άλλα συστατικά.
- Return Error: Reports the unsuccessful completion of an invoked operation.
- Reject: Indicates that an incorrect package type or component was received.

Τα συστατικά(components) περιλαμβάνουν τις παραμέτρους που περιέχουν τα οριζόμενα από την εφαρμογή στοιχεία, μεταφέρονται ανεξέταστα από το TCAP. Η δομή του header του TCAP είναι η ακόλουθη:



- Information Element - Ένα στοιχείο πληροφοριών ερμηνεύεται αρχικά σύμφωνα με τη θέση του μέσα στη σύνταξη του μηνύματος. Κάθε στοιχείο πληροφοριών μέσα σε ένα μήνυμα TCAP έχει την ίδια δομή. Ένα στοιχείο

πληροφοριών αποτελείται από τρεις τομείς: Ετικέτα (Tag), μήκος και περιεχόμενο.

- Tag - Η ετικέτα διακρίνει ένα στοιχείο πληροφοριών από ένα άλλο και ελέγχει την ερμηνεία του περιεχομένου. Μπορεί να είναι ένα ή περισσότερα octets στο μήκος. Η ετικέτα αποτελείται από τους Class, Form και Tag κωδικούς.
- Length - Διευκρινίζει το μήκος του περιεχομένου.
- Contents - Περιέχει την ουσία του στοιχείου, που περιέχει τις αρχικές πληροφορίες που το στοιχείο προορίζεται να μεταβιβάσει.

Το transaction ID είναι μια αναφορά TCAP για ένα σύνολο διαδικασιών TCAP που εκτελούνται μέσα σε έναν ενιαίο διάλογο. Όταν η μηχανή Α αρχίζει έναν διάλογο TCAP με μια άλλη μηχανή Β, η μηχανή Α στέλνει ένα Begin μήνυμα στη μηχανή Β. Αυτό το Begin μήνυμα περιέχει το Originating Transaction ID, η οποία είναι η αναφορά του Transaction ID για το Α. Όταν η μηχανή Β απαντά στο Α με ένα Continue μήνυμα περιλαμβάνει ένα Transaction ID ως Destination Transaction ID. Επιπλέον το Β περιλαμβάνει το Transaction ID του ως το Originating Transaction ID.

Καθώς ο διάλογος TCAP πηγαίνει σε κάθε Continue μήνυμα περιλαμβάνει το Transaction ID της μηχανής προορισμού ως Destination Transaction ID και το Transaction ID της μηχανής προορισμού ως Originating Transaction ID. Όταν οποιαδήποτε από τις μηχανές θέλει να κλείσει το διάλογο στέλνει ένα μήνυμα τέλους ή ένα μήνυμα ακύρωσης στην άλλη μηχανή. Αυτό το μήνυμα περιέχει μόνο το Destination Transaction ID.

3.3.4 Mobile Terminated SMS

Εάν το δίκτυο που εξυπηρετεί (serving network) λάβει ένα mt-forward-SM MAP μήνυμα που χρησιμοποιεί το TC_Continue για να μεταφέρει το MAP ωφέλιμο φορτίο, είναι εγγυημένο ότι το SCCP θα καλεί τη διεύθυνση όλων των συμβαλλόμενων μερών (party address) να μάθει αν το TC_Begin μήνυμα είναι αυθεντικό, διαφορετικά το πρώτο TC-continue μήνυμα θα στελνόταν στην πλαστή διεύθυνση. Η σωστή ροή μηνυμάτων εγγυάται από τις δυνατότητες συναλλαγής

TCAP (χρήση του Transaction ID). Δυστυχώς υπάρχουν μερικοί τρόποι με τους οποίους μια ψευδής SMS Gateway μπορεί να προσπαθήσει να παρακάμψει την υπονοούμενη επικύρωση διευθύνσεων SCCP που παρέχεται από τη χειραψία TCAP.

- Ο δημιουργός(originator) περιλαμβάνει μια πλαστή διεύθυνση SMS-GMSC σαν SM-RP-OA στο ωφέλιμο φορτίο του mt-forward-SM που φέρεται από το TC-continue.
- Ο δημιουργός προσπαθεί να προβλέψει το TCAP transaction ID που ορίζεται από τον κόμβο εξυπηρετητή, ο οποίος είναι να χρησιμοποιηθεί μέσα στο τρίτο μήνυμα, και υποκρίνετε (spoofs) το τρίτο μήνυμα χωρίς αναμονή για το δεύτερο μήνυμα. Αυτή η επίθεση πρέπει να πραγματοποιηθεί μέσα στο σωστό χρονικό παράθυρο.

Εάν η χειραψία TCAP(handshake) πρόκειται να χρησιμοποιηθεί, το ακόλουθο μέτρο θα ληφθεί μέσα στο δίκτυο του εξυπηρετητή κόμβου προκειμένου να αντιδράσουν στις δυνατότητες υποκρισίας ενός κακόβουλου δημιουργού ενός mt-Forward-SM.

- MEAS-1: Το λαμβάνουν δίκτυο (receiving network) θα ελέγξει εάν η λαμβανόμενη διεύθυνση SMS-GMSC (ως SM-RP-OA στο τρίτο μήνυμα) μπορεί να χρησιμοποιηθεί από το SCCP Calling Party Address. Μερικοί πάροχοι χρησιμοποιούν μια ενιαία διεύθυνση SMS-GMSC για μια σειρά SCCP Calling Party Addresses και αυτό θα πρέπει να ληφθεί υπόψη.

Εάν η χειραψία TCAP πρόκειται να χρησιμοποιηθεί, τουλάχιστον ένα από τα ακόλουθα μέτρα θα ληφθεί μέσα στο δίκτυο του εξυπηρετητή κόμβου προκειμένου να αντιμετωπιστούν οι δυνατότητες υποκρισίας(spoofing) ενός κακόβουλου δημιουργού ενός mt-Forward-SM.

- MEAS-2a: Ο λαμβάνων κόμβος θα χρησιμοποιήσει τους μηχανισμούς για να εξασφαλίσει ότι το TCAP transaction ID του προορισμού TCAP που πρέπει να χρησιμοποιηθεί μέσα στο τρίτο μήνυμα είναι προβλέψιμη με μια πιθανότητα λιγότερο από 1/210 για έναν τρίτο που ξέρει όλες τις προηγούμενες τιμές του TCAP transaction ID.

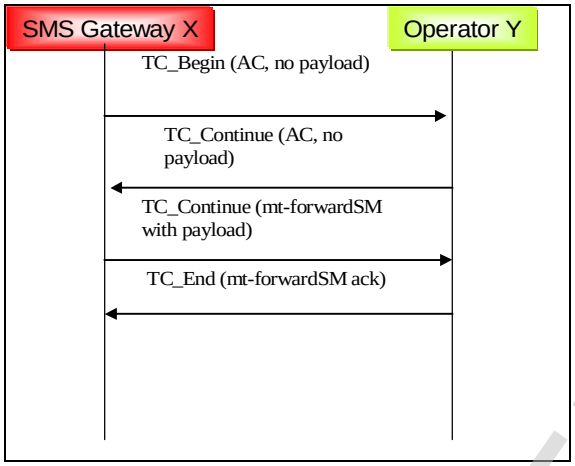
- MEAS-2b: Το λαμβάνον δίκτυο θα περιμένει τα ν δευτερόλεπτα προτού να επεξεργαστεί το τρίτο μήνυμα (TC-continue(mt-forwardSM με ωφέλιμο φορτίο)). Αυτό πρέπει να εξασφαλίσει ότι το TC_abort από το δίκτυο υποβάλλεται σε επεξεργασία στον κόμβο προορισμού νωρίτερα από ένα TC_continue συμπεριλαμβανομένης μιας επιτυχής πρόβλεψης για την αξία ενός TCAP Transaction ID.

Η ακόλουθη μέθοδος ομαδοποίησης μπορεί να χρησιμοποιηθεί για έναν πάροχο για να εισαγάγει βαθμιαία τη χειραψία(handshake) TCAP για τα μηνύματα mt-Forward-SM. Καθορίστε έναν «πάροχο ομάδα-1» ως εμπιστευμένη ομάδα χειριστών και «πάροχο ομάδα -2»ως μη εμπιστευμένη ομάδα χειριστών. Συμφωνήστε ότι ομάδα-1 χρησιμοποιεί τη χειραψία TCAP, ενώ ομάδα-2 δεν χρησιμοποιούν τη χειραψία TCAP. Οι χειριστές του SMS Gateway που ανήκουν σε ομάδα-1 είτε θα χρησιμοποιήσουν την εφαρμογή context2 είτε 3 για το mt-Forward-SM. Η διαχείριση των δύο ομάδων απαιτεί ότι το εξυπηρετώντας δίκτυο θα εφαρμόσει έναν πίνακα (policy table) του SCCP Calling Party Addresses για τις οποίες μια χειραψία TCAP απαιτείται.

Εάν η πιο πάνω μέθοδος ομαδοποίησης χρησιμοποιείται, έπειτα το ακόλουθο μέτρο θα ληφθεί στο δίκτυο εξυπηρετητή (serving network) προκειμένου να αντιδράσουν στην πιθανότητα υποκρισίας(spoofing) ενός κακόβουλου δημιουργού ενός mt-Forward-SM που προσπαθεί να παρακάμψει τους ελέγχους στους πίνακες (policy table).

- MEAS-3: Το δίκτυο εξυπηρετητή θα ελέγξει ότι το SCCP Calling Party Address ενός πρώτου μηνύματος με ένα ωφέλιμο φορτίο (δηλ. χωρίς να χρησιμοποιήσει τη χειραψία TCAP) δεν είναι από μια SMS-GMSC - διεύθυνση όπως το SM-RP-OA που θα χρησιμοποιήσει τη χειραψία TCAP.

Το όφελος που αποκομίζεται για τους χειριστές που ανήκουν στην ομάδα-1 είναι ότι το spoofing των SMS-GMSC-addresses τους είναι σχεδόν δύσκολη εάν ο πίνακας (policy table) έχει διαχειριστεί σωστά.



MAP mt-Forward-SM μηνύματα με χρήση TCAP Handshakes

3.3.5 Mobile Originated SMS

Εάν το δίκτυο εξυπηρετητή (serving network) στέλνει ένα mo-forward-SM MAP μήνυμα που χρησιμοποιεί το TC_Continue για να μεταφέρει το ωφέλιμο φορτίο MAP έπειτα αυτό είναι εγγυημένο ότι το SCCP calling party του (κενού) TC_Begin είναι αυθεντικό, διαφορετικά το πρώτο TC-continue μήνυμα θα στελνόταν στην πλαστή διεύθυνση. Η σωστή ροή μηνυμάτων εγγυάται από τις δυνατότητες συναλλαγής TCAP (χρήση του Transaction ID). Δυστυχώς υπάρχουν μερικοί τρόποι με τους οποίους ένας χειριστής ψευδής υπηρεσία (MSC ή SGSN) μπορεί να προσπαθήσει να παρακάμψει την υπονοούμενη επικύρωση διευθύνσεων SCCP που παρέχεται από τη χειραψία TCAP.

- Ο δημιουργός περιλαμβάνει ένα πλαστό MSISDN σαν SM-RP-OA μέσα στο ωφέλιμο φορτίο του mo-forward-SM που μεταφέρεται από το TC-continue .
- Ο δημιουργός προσπαθεί να προβλέψει το TCAP transaction ID που ορίζεται από τον εξυπηρετητή κόμβο, το οποίο είναι να χρησιμοποιηθεί μέσα στο τρίτο μήνυμα, και παραποιεί (spoofs) το τρίτο μήνυμα χωρίς αναμονή για το δεύτερο μήνυμα. Αυτή η επίθεση πρέπει να πραγματοποιηθεί μέσα στο σωστό χρονικό διάστημα.

Εάν η χειραψία TCAP πρόκειται να χρησιμοποιηθεί, το ακόλουθο μέτρο μπορεί να ληφθεί μέσα στο δίκτυο του SMS Interworking MSC προκειμένου να

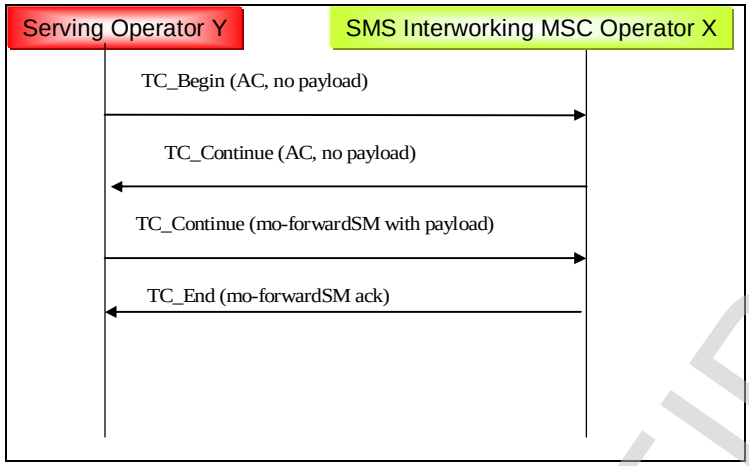
αντιδράσουν οι δυνατότητες spoofing ενός κακόβουλου δημιουργού mo-Forward-SM.

- MEAS-1: Ο λαμβάνων κόμβος (δηλ. το SMS interworking MSC) μπορεί να κάνει το query στο HLR για να ελέγξει εάν το λαμβανόμενο SCCP Calling Party Address του mo-forward-SM είναι από το ίδιο δίκτυο που εξυπηρετεί αυτήν την περίοδο το συνδρομητή (MSISDN που περιλαμβάνεται στο SM-RP-OA στο τρίτο μήνυμα).

Η ακόλουθη μέθοδος ομαδοποίησης μπορεί να χρησιμοποιηθεί για έναν χειριστή για να εισαγάγει βαθμιαία τη χειραψία TCAP για τα μηνύματα mo-Forward-SM. Καθορίστε μια "ομάδα χειριστών -1" ως εμπιστευμένη ομάδα χειριστών και "το ομάδα χειριστών -2" ως μη εμπιστευμένη ομάδα χειριστών. Συμφωνήστε ότι η ομάδα-1 χρησιμοποιεί τη χειραψία TCAP, ενώ ομάδα-2 δεν χρησιμοποιούν τη χειραψία TCAP. Οι χειριστές του MSC που ανήκουν στην ομάδα-1 είτε θα χρησιμοποιήσουν την εφαρμογή context2 είτε 3 για το mo-Forward-SM. Η διαχείριση των δύο ομάδων απαιτεί ότι το δίκτυο του SMS Interworking MSC θα εφαρμόσει έναν πίνακα(policy table) με τις SCCP-addresses για τις οποίες μια χειραψία TCAP απαιτείται. Εάν η ανωτέρω περιγραμμένη μέθοδος ομαδοποίησης χρησιμοποιείται έπειτα το ακόλουθο μέτρο θα ληφθεί στο SMS Interworking MSC προκειμένου να αντιμετωπιστούν οι δυνατότητες υποκρισίας(spoofing) ενός κακόβουλου δημιουργού ενός mo-Forward-SM που προσπαθεί να παρακάμψει τους ελέγχους των πινάκων.

- MEAS-3: Το SMS Interworking MSC θα ελέγξει ότι το SCCP Calling Party address ενός πρώτου μηνύματος με ένα ωφέλιμο φορτίο (δηλ. μην χρησιμοποιώντας τη χειραψία TCAP) δεν είναι από μια διεύθυνση που θα χρησιμοποιήσει τη χειραψία TCAP.

Το όφελος που αποκομίζεται για τους χειριστές που ανήκουν σε ομάδα-1 είναι ότι η υποκρισία(spoofing) ενός mo-Forward-SM για τους συνδρομητές τους, ενώ κάνουν roaming μέσα σε μια ομάδα-1, γίνεται σχεδόν δύσκολη εάν ο πίνακας έχει διαχειριστεί σωστά.



MAP mo-Forward-SM μηνύματα με χρήση TCAP Handshakes

3.4 Παρεμπόδιση των Multimedia Messaging Service (MMS)

Η αλλαγή αυτή έχει παρουσιαστεί στις προδιαγραφές του UMTS έκδοση 6. Η αλλαγή είναι στο “Technical Specification Group Services and System Aspects; 3G Security; Lawful interception architecture and functions. (33107)”.

3.4.1 Multimedia Messaging Service (MMS)

Η υπηρεσία μηνύματος πολυμέσων (mms) είναι ένα πρότυπο για τα συστήματα τηλεφωνικών μηνυμάτων που επιτρέπουν μηνύματα που περιλαμβάνουν αντικείμενα πολυμέσων (εικόνες, ακουστικό, τηλεοπτικό, rich text) και όχι μόνο το κείμενο όπως στο Short Message Service (SMS). Επεκτείνεται κυρίως στα κυψελοειδή (cellular)δίκτυα μαζί με άλλα συστήματα μηνύματος όπως το SMS, το Mobile Instant Messaging και το κινητό ηλεκτρονικό ταχυδρομείο. Η κύρια προσπάθεια τυποποίησής της γίνεται από τα 3GPP, 3GPP2 και την Open Mobile Alliance (OMA).

Στις αρχές της δεκαετίας του '80 μια ομάδα προμηθευτών numerical controller (NC), κατασκευαστών μηχανημάτων και χρηστών που εργάζονταν υπό την αιγίδα της επιτροπής IE31 της βορειοαμερικανικής Electronic Industries Association (EIA) είχε αναπτύξει ένα draft με τον τίτλο το "User Level Format and Protocol for Bidirectional Transfer of Digitally Encoded Information in a Manufacturing Environment". Η

κατάσταση στην αυτοματοποίηση κατασκευής εκείνη την περίοδο (δηλ. στα μέσα της δεκαετίας του '80) ήταν ένας βιομηχανικός πύργος της Βαβέλ. Κάθε τομέας της αυτοματοποίησης είχε την ιδιοσυγκρασία της στον τρόπο που έβλεπε τα πράγματα, και οι παραλλαγές της ορολογίας μεταξύ των προμηθευτών εξοπλισμού προσέθεταν στη σύγχυση.

Όταν η εταιρία General Motors άρχισε την προσπάθεια του Manufacturing Automation Protocol (MAP) το 1980, χρησιμοποίησαν την πρόταση προτύπων σχεδίων του EIA- 1393A ως βάση για ένα γενικότερο πρωτόκολλο μηνύματος που θα μπορούσε να χρησιμοποιηθεί για NCs, programmable logic controllers (PLC), τα ρομπότ και άλλες ευφυείς συσκευές που χρησιμοποιήθηκαν συνήθως στα περιβάλλοντα μιας κατασκευής. Το αποτέλεσμα ήταν το π the Manufacturing Message Format Standard (MMFS). Το MMFS χρησιμοποιήθηκε στις προδιαγραφές του MAP Version 2 που δημοσιεύθηκαν σε 1984. Κατά τη διάρκεια της αρχικής χρήσης του MMFS έγινε προφανές ότι αυστηρότερα πρότυπα μηνύματος απαιτήθηκαν. Το MMFS επέτρεψε πάρα πολλές επιλογές για τους υπεύθυνους για την ανάπτυξη συσκευών και εφαρμογής. Αυτό οδήγησε σε διάφορες συνήθως ασυμβίβαστες διαλέκτους του MMFS. Επιπλέον, το MMFS δεν παρείχε ικανοποιητική λειτουργία για να είναι χρήσιμο για τα Process Control Systems (PCS) που βρέθηκαν στις συνεχείς βιομηχανίες επεξεργασίας. Με στόχο την ανάπτυξη ενός συστήματος γενικού και όχι για τη βιομηχανία συγκεκριμένα για τις επικοινωνίες μεταξύ των ευφυών συσκευών κατασκευής της MMS προσπάθειας που άρχισε υπό την αιγίδα του ISO TC 184.

Το αποτέλεσμα ήταν ένα πρότυπο που βασίστηκε στο Open Systems Interconnection (OSI) μοντέλο, αποκαλούμενο και Manufacturing Message Specification (MMS). Μια Draft International Standard (DIS) έκδοση του MMS δημοσιεύθηκε τον Δεκέμβριο του 1986 ως ISO DIS 9506. Η DIS έκδοση του MMS (έκδοση 0) υπερνίκησε τα προβλήματα με το MMFS αλλά δεν ήταν προωθημένη ακόμα στη θέση ενός International Standard (IS). Αντιμέτωπες με μια προθεσμία για να δημοσιεύσουν έως τον Νοεμβρίου του 1988 οι Τεχνικές Επιτροπές MAP παρέπεμψαν την έκδοση DIS του MMS για την προδιαγραφή του MAP V3.0. Το Δεκέμβριο του 1988 η IS έκδοση του MMS (έκδοση 1) κυκλοφόρησε ως ISO 9506 μέρος 1 και 2.

Όπως με τα περισσότερα 3GPP πρότυπα, τα MMS πρότυπα έχουν τρία στάδια:

- Stage 1 - Απαιτήσεις (Requirements) (3GPP TS 22.140)
- Stage 2 - Λειτουργίες Συστήματος (System Functions) (3GPP TS 23.140)
- Stage 3 - Τεχνικές Πραγματοποιήσεις (Technical Realizations)

Οι βασικές αρχές του SMS και του MMS είναι παρόμοιες, αλλά η διαφορά στο περιεχόμενο είναι δραματική. Το μέγεθος ενός μέσου μηνύματος SMS είναι περίπου 140 bytes, ενώ στα αρχικά στάδιά του, το μέσο μέγεθος ενός MMS μηνύματος είναι πιθανό να είναι περίπου 30.000 bytes, και αργότερα, περίπου 100.000 bytes. Τα στοιχεία των μηνυμάτων είναι διαθέσιμα στους χρήστες ως τμήμα του MMS εξαρτώνται από τις ικανότητες για τη διαχείριση των δεδομένων του ασύρματου δικτύου και από τις ικανότητες της συσκευής. Δεδομένου ότι τα κινητά δίκτυα αναπτύσσονται (τρίτης γενιάς), και οι νέες κινητές συσκευές εισάγονται, η σειρά των επιλογών μηνύματος θα αυξηθεί.

Οι ακόλουθες επιλογές μηνυμάτων καλύπτονται αυτήν την περίοδο από τα MMS πρότυπα. Περισσότερα θα προστεθούν καθώς τα πρότυπα αναπτύσσονται:

Το κείμενο όπως με το SMS και το EMS, σε ένα MMS μήνυμα μπορεί να αποτελείτε από το απλό κείμενο (plain text). Το EMS και το MMS επιτρέπουν επίσης στο κείμενο να σχηματοποιηθεί χρησιμοποιώντας διαφορετικές πηγές, μεγέθη και μορφές. Η κύρια διαφορά μεταξύ του σχηματοποιημένου κειμένου στο EMS και το MMS είναι ότι το MMS επιτρέπει πολύ μεγαλύτερα ποσά κειμένου από το SMS/EMS.

Στο EMS, το σχηματοποιημένο κείμενο(formatted text) μπορεί να συνοδευθεί από απλές εικόνες ή μελωδίες. Στο MMS, το σχηματοποιημένο κείμενο μπορεί να συνοδευθεί από φωτογραφικές εικόνες, γραφική παράσταση, ακουστικά δείγματα, και τηλεοπτικές ακολουθίες.

Οι γραφικές παραστάσεις, οι πίνακες, τα διαγράμματα, οι χάρτες, τα σκίτσα, τα σχέδια και τα σχεδιαγράμματα γραφικής παράστασης είναι ακριβώς μερικά παραδείγματα του είδους γραφικής παράστασης που το MMS μπορεί να χειριστεί. Δεδομένου ότι οι βασισμένες στη θέση (location-based) υπηρεσίες γίνονται

περισσότεροι επικρατούσες, οι χάρτες και τα σκίτσα θα έχουν πάντα μεγαλύτερη σχετικότητα στους κινητούς χρήστες.

Τα coding formats της εικόνας που χρησιμοποιούνται στα MMS μηνύματα είναι:

- γραμμή βάσεων (base line) JPEG με JFIF ως σχήμα ανταλλαγής(exchange format)
- GIF87a
- GIF89a
- WBMP
- JPEG 2000
- 60 x 80 pixels
- 120 x 160 pixels
- 240 x 320 pixels

Η μέγιστη ανάλυση εικόνας για την οποία η διαλειτουργικότητα είναι εγγυημένη είναι 240x320 pixels.

Τα ακουστικά δείγματα του MMS υποστηρίζουν την προσθήκη των ακουστικών δειγμάτων στα μηνύματα. Παραδείγματος χάριν, οι χρήστες μπορούν να ανταλλάξουν ένα αγαπημένο τραγούδι, ή μπορούν να χρησιμοποιήσουν το κινητό τηλέφωνο για να καταγράψουν και να στείλουν τα δείγματα ήχου, συμπεριλαμβανομένης της φωνής. Για τους MMS πελάτες που υποστηρίζουν ήχο από ομιλία ή πολυμέσα, το coding format που χρησιμοποιείται από τα MMS στα μηνύματα είναι:

- MP3
- MIDI
- WAV

Οι συγχρονισμένες παρουσιάσεις χρησιμοποιούν τη γλώσσα synchronized multimedia integration language (SMIL, ένα βασισμένο στο XML πρωτόκολλο), το MMS έχει τις PowerPoint -ύφους παρουσιάσεις (με ήχο και εικόνα) για να δημιουργηθεί και να σταλεί από και προς τις κινητές συσκευές. Χρησιμοποιώντας έναν απλό συντάκτη πολυμέσων, οι χρήστες μπορούν να ενσωματώσουν ήχο και

βίντεο μαζί με τις εικόνες και το σχηματοποιημένο κείμενο στις παρουσιάσεις πολυμέσων.

Το βίντεο είναι η τελευταία επέκταση του MMS που οι ψηφιακές ικανότητες απεικόνισης θα είναι τηλεοπτικό περιεχόμενο. Οι χρήστες θα είναι σε θέση να καταγράψουν μια σκηνή χρησιμοποιώντας μια ενσωματωμένη ψηφιακή φωτογραφική μηχανή και να διαβιβάσουν το clip σε έναν παραλήπτη (αρχικά, θα είναι σε θέση να ανταλλάξουν 30-δεύτερων video clips).

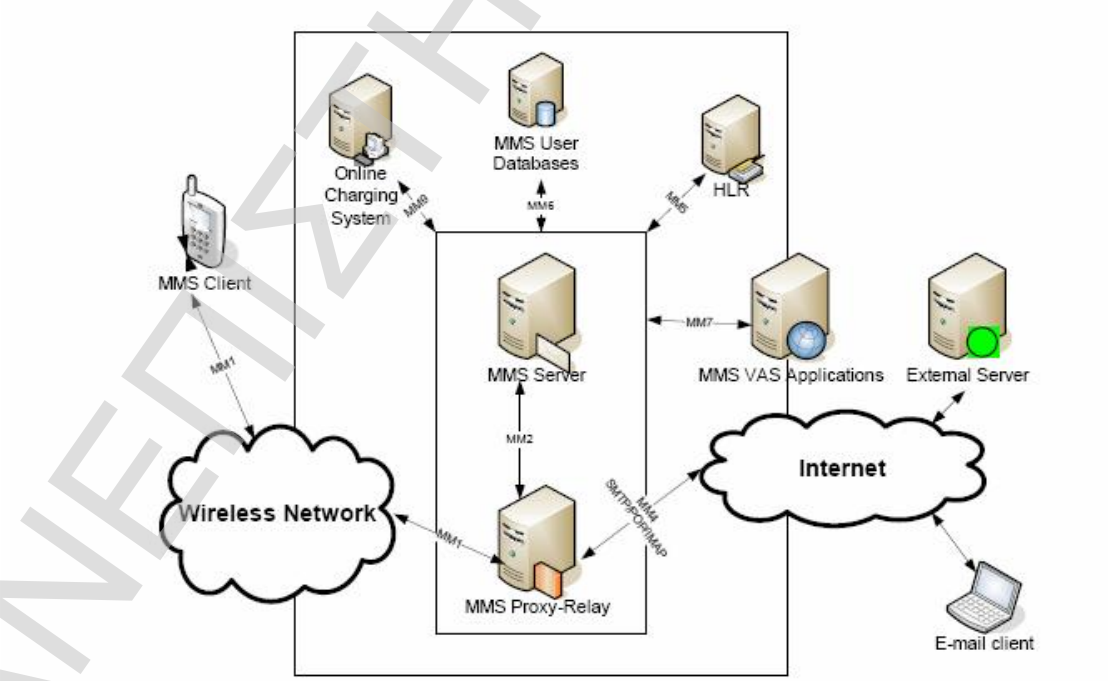
Για τους MMS πελάτες που υποστηρίζουν τον τύπο μέσων του βίντεο, το coding format που χρησιμοποιείται στα MMS μηνύματα είναι:

- ITU-T H.263
- MPEG 4
- (Simple Profile)
- Quicktime
- Third-generation Partnership Project (3GPP)

Το streaming τηλεοπτικό και ακουστικό περιεχόμενο μπορεί να δοθεί (streamed) χρησιμοποιώντας το MMS χωρίς να πρέπει να καταληφθεί η μνήμη στο τηλέφωνο. Αν και αυτό φαίνεται όπως μια αντίφαση δεδομένου ότι η βασική αρχή του MMS είναι να αποθηκευτούν τα μηνύματα τοπικά στην τεχνολογία του Phone streaming, είναι πραγματικά καλά ταιριασμένο για το MMS. Όταν το μήνυμα αντιμετωπίζεται στο τηλέφωνο, το περιεχόμενο δεν αποθηκεύεται, αλλά δίνετε άμεσα σε το.

Το MMS σχεδιάστηκε πρώτιστα ως person-to-person υπηρεσία για τα μηνύματα πολυμέσων. Το MMS τυποποιείται από το 3G Partnership πρόγραμμα και την Open Mobile Alliance. Είναι ουσιαστικά ένα store and forward σύστημα μηνυμάτων, παρόμοιο γενικά σε σχέδιο με το SMS. Ο χρήστης υποβάλλει ένα μήνυμα σε ένα κέντρο μηνυμάτων, όπου αποθηκεύεται και στέλνεται σε έναν άλλο χρήστη όταν είναι εφικτό αυτό. Οι λεπτομέρειες, εντούτοις, είναι αρκετά διαφορετικές από το SMS. Τα κύρια συστατικά της MMS αρχιτεκτονικής παρουσιάζονται στο σχήμα.

Το MMS Relay/Server μπορεί να αντιμετωπισθεί ως ενιαίο φυσικό συστατικό στην αρχιτεκτονική, ακόμα κι αν αποτελείται από δύο χωριστές λογικές οντότητες δικτύων - το MMS Proxy-Relay και το MMS Server. Ο MMS Proxy-Relay δια-κωδικοποιεί και παραδίδει τα μηνύματα. Είναι αρμόδιο για τη μεταφορά των μηνυμάτων μεταξύ των διαφορετικών συστημάτων μηνύματος. Εκτελεί την ανάκτηση των διευθύνσεων, τη δρομολόγηση, συλλέγει τις πληροφορίες χρέωσης, εκτελεί την προσαρμογή του περιεχομένου και μετατρέπει τα formats των μηνυμάτων εάν είναι απαραίτητο. Ο MMS Server είναι μια αποθήκη μηνυμάτων. Δεδομένου ότι το MMS είναι ένα store and forward σύστημα μηνύματος, ο MMS Server θα είναι όπου τα μηνύματα κρατούνται αναμένοντας τους σωστούς όρους για την παράδοση ή τη μεταφορά.
Ο MMS Server έχει συχνά μια διεπαφή Ιστού για την ανάκτηση των μηνυμάτων.
Ούτε το 3GPP ούτε το WAP φόρουμ δεν διευκρινίζει μια διεπαφή μεταξύ του MMS Proxy-Relay και του MMS Server. Για αυτόν τον λόγο τα διαφορετικά επιχειρησιακά πρότυπα μπορούν να οδηγήσουν στο διαφορετικό partitioning ή συνδυασμούς αυτών των δύο. Από κοινού καλούνται μερικές φορές MMSC. Ο MMS User Agent, ή MMS Client στις προδιαγραφές OMA, είναι το συστατικό που αλληλεπιδρά με το χρήστη. Πρέπει να παρέχει τα μέσα για δημιουργία και αποστολή των μηνυμάτων πολυμέσων. Χαρακτηριστικά, αυτό θα είναι ένα κινητό τηλέφωνο.



MMS Αρχιτεκτονική

Η MMS User Database περιέχει τις περιγραφές και τα σχεδιαγράμματα χρηστών, που περιέχουν τις πληροφορίες για τις συνδρομές και τις διαμορφώσεις. Το Home Location Register (HLR) είναι μια άλλη βάση δεδομένων, που περιέχει τις πληροφορίες για τους συνδρομητές. Το online σύστημα χρέωσης είναι αρμόδιο για τον έλεγχο εάν ένας συνδρομητής έχει την άδεια για να χρησιμοποιήσει έναν ορισμένο πόρο δικτύων. Αυτό είναι ιδιαίτερα σημαντικό στις προπληρωμένες υπηρεσίες όπου χρησιμοποιείται για να καθορίσει εάν ένας συνδρομητής έχει ή όχι αρκετή πίστωση για να ολοκληρώσει τη MMS συναλλαγή. Το MMS Value Added Services (VAS) της MMS αρχιτεκτονικής είναι σημαντικό στα πλαίσια του δημιουργημένου από το χρήστη περιεχομένου. Ένα VAS ορίζεται ως μια υπηρεσία που μπορεί να παρέχει στο χειριστή το πρόσθετο εισόδημα και τον πελάτη με μια πρόσθετη υπηρεσία χωρίς μείωση των κερδών από τη βασική υπηρεσία. Μια εφαρμογή VAS μπορεί να παραγάγει τα Call Data Records (CDRs) όταν λαμβάνετε ένα MMS από το Proxy-Relay, αυτά τα το CDRs στέλνονται στο online σύστημα χρέωσης.

3.4.1 Παρεμπόδιση του Multimedia Messaging Service (MMS)

Το Multimedia Messaging Service (MMS) είναι μια υπηρεσία που τρέχει πέρα από την 3GPP PS-domain. Και τα MMS που δημιουργούνται αλλά και αυτά που ολοκληρώνονται στα κινητά πρέπει να περάσουν μέσω των PS domain GSN κόμβων καθοδόν σε ή από τα Multimedia Message Service Centres (MMSCs). Επομένως, η παρεμπόδιση των MMS μηνυμάτων θα εκτελεστεί στο GSN με ακριβώς τον ίδιο τρόπο όπως για άλλες υπηρεσίες φορέων του PS-domain. Το GSN δεν είναι αρμόδιο για την ανάκτηση των μεμονωμένων MMS μηνυμάτων από το IP stream.

3.5 Υποστήριξη των A5 Αλγορίθμων στους Κινητούς Σταθμούς (mobile stations)

Η αλλαγή αυτή έχει παρουσιαστεί στις προδιαγραφές του UMTS έκδοση 6. Η αλλαγή είναι στο “Technical Specification Group Services and system Aspects; Security related network functions (43020)”.

3.5.1 Κινητοί Σταθμοί (mobile stations)

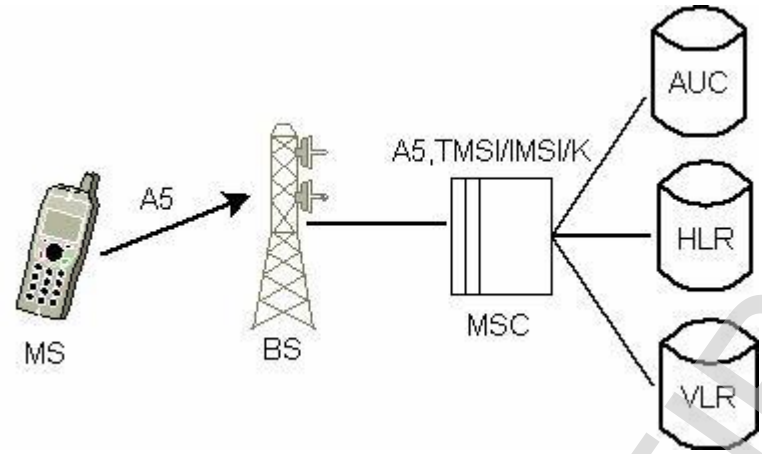
Ο κινητός σταθμός (MS) περιλαμβάνει όλους τον εξοπλισμό και το λογισμικό χρηστών που απαιτούνται για την επικοινωνία με ένα ασύρματο τηλεφωνικό δίκτυο. Το MS αναφέρεται σαν κινητό τηλέφωνο, το τηλέφωνο που κατέχουν οι χρήστες στο κινητό δίκτυο. Αυτό είναι η ορολογία των 2G συστημάτων όπως το GSM. Στα 3G συστήματα, το MS αναφέρεται τώρα ως εξοπλισμός χρηστών (User Equipment UE).

Ο εξοπλισμός χρηστών είναι η φυσική συσκευή που χρησιμοποιείται από τους χρήστες. Αποτελείται από έναν κινητό εξοπλισμό (ME) και ένα UMTS Subscriber Identity Module(USIM). Το USIM είναι μια εφαρμογή που αποθηκεύεται στις υπηρεσίες σε μια μετακινούμενη κάρτα ολοκληρωμένου κυκλώματος που επικοινωνεί με το ME για να παρέχει πρόσβαση στο 3G.

3.5.2 Αλγόριθμος A5

Ο A5 αλγόριθμος είναι ένας stream cipher αλγόριθμος. Εφαρμόζεται πολύ αποτελεσματικά στο hardware και το σχέδιο του δεν δημοσιοποιήθηκε ποτέ. Υπάρχουν 3 διαφορετικές εκδόσεις του A5: A5/1 - οι ισχυρές εκδόσεις, A5/2 -μια αδύνατη έκδοση και A5/3 - βασισμένο στους αλγορίθμους που χρησιμοποίησαν τα τηλέφωνα 3G. Υπάρχει επίσης το A5/0 αλλά δεν έχει καμία κρυπτογράφηση.

Αυτοί οι αλγόριθμοι μπορούν επίσης να σπάσουν αρκετά εύκολα. Με την ανάλυση της εξόδου του A5/1 για 2 λεπτά μπορεί να σπάσει σε λιγότερο από ένα δευτερόλεπτο. Ο πιο αδύνατος A5/2 αλγόριθμος μπορεί να σπάσει στα χιλιοστά του δευτερολέπτου και οι επιθέσεις ενάντια στο A5/3 έχουν περιγραφεί.



A5 κρυπτογράφηση σε GSM δίκτυο

3.5.2.1 Αλγόριθμος A5/1

Ο A5/1 είναι ένας stream cipher αλγόριθμος που χρησιμοποιείται για να παρέχει την ιδιωτικότητα της φωνής στο ασύρματο δίκτυο στα κυψελοειδή τηλεφωνικά πρότυπα GSM. Κρατήθηκε αρχικά μυστικός, αλλά έγινε δημόσια γνωστός μέσω των διαρροών και της αντίστροφης εφαρμοσμένης μηχανικής(reverse engineering). Διάφορες σοβαρές αδυναμίες στην κρυπτογράφηση έχουν προσδιοριστεί.

Μια επισκόπηση του αλγορίθμου:

- Input: 64-bit μυστικό κλειδί Kc, 22-bit γνωστό σαν IV Fn
- Output: Δύο 114-bit blocks of keystream χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων.
- Data: Πληροφορία signaling η 5 ms από την ψηφιακά κωδικοποιημένη ομιλία
- Encryption: Bitwise exclusive-or (XOR)

3.5.2.2 Αλγόριθμος A5/2

Ο A5/2 είναι ένας stream cipher αλγόριθμος που χρησιμοποιείται για να παρέχει την ιδιωτικότητα φωνής στο κυψελοειδές τηλεφωνικό πρωτόκολλο GSM. Ο A5 αλγόριθμος χρησιμοποιείται στο GSM λογαριάζοντας τη διαδικασία μεταξύ ενός MS (Mobile Station) και του δικτύου GSM. Αυτός ο αλγόριθμος είναι απλούστερος από τον A5/1 και αναπτύχθηκε από το ETSI (European Telecommunications Standards

Institute) για χρήση στα ανατολικο-ευρωπαϊκά κράτη που είχαν τους περιορισμούς σε ορισμένες δυτικές τεχνολογίες.

Η κρυπτογράφηση είναι βασισμένη περίπου έναν συνδυασμό τεσσάρων γραμμικών καταλόγων μετατόπισης ανατροφοδότησης(four linear feedback shift registers) με την ανώμαλη χρονομέτρηση(irregular clocking) και έναν μη γραμμικό συνδυαστή (non-linear combiner).

Το 1999, ο Ian Goldberg και ο David Wagner κρυπταναλύσανε τον A5/2 και τον ίδιο μήνα δημοσιεύθηκε και έδειξε ότι ήταν εξαιρετικά αδύνατο - σε τόσο μεγάλο μέρος έτσι ώστε ένας χαμηλού επιπέδου εξοπλισμός μπορεί πιθανώς να το σπάσει σε πραγματικό χρόνο.

Συμφωνώντας με το GSMA (GSM Association) από την 1η Ιουλίου του 2006, τα κινητά τηλέφωνα δεν θα υποστηρίξουν άλλο με τον αλγόριθμο A5/2, που αναπτύσσεται κυρίως για τις χώρες της Ασίας, δεδομένου ότι ο κώδικας έσπασε το 1999, και εν πάση περιπτώσει ο A5/1 είναι ισχυρότερος από τον A5/2, και υποστηρίζεται σαν υποχρεωτικό, από τη 3GPP ένωση.

3.5.2.3 Αλγόριθμος A5/3 (KASUMI)

Ο KASUMI αλγόριθμος, που καλείται επίσης και A5/3, είναι block cipher αλγόριθμος που χρησιμοποιείται στην εμπιστευτικότητα (f8) και τους αλγορίθμους ακεραιότητας (f9) για το 3GPP την κινητή επικοινωνία. Ο KASUMI σχεδιάστηκε από το Security Algorithms Group of Experts (SAGE), μέρος του ευρωπαϊκού οργανισμού προτύπων, ETSI. Παρά να εφευρεθεί μια κρυπτογράφηση από την αρχή, ένας υπάρχων αλγόριθμος, ο MISTY1, επιλέχτηκε από το SAGE και βελτιστοποιήθηκε ελαφρώς για την εφαρμογή στο hardware. Ως εκ τούτου, και ο MISTY1 και ο KASUMI είναι πολύ παρόμοιοι και η κρυπτολογική ανάλυση του ενός είναι πιθανό να είναι εύκολα προσαρμόσιμη στον άλλο.

Ο KASUMI έχει ένα block size 64 bits και ένα μέγεθος κλειδιού 128 bits. Είναι ένας cipher Feistel με οκτώ κύκλους, και όπως τα MISTY1 και MISTY2, έχει μια

επαναλαμβανόμενη δομή, με τα μικρά εξαρτήματα επίσης που έχουν μια Feistel - ομοειδή μορφή.

Το 2001, μια αδύνατη διαφορική επίθεση σε έξι κύκλους στο KASUMI παρουσιάστηκε από τον Kühn (2001).

Το 2005, οι ισραηλινοί ερευνητές Eli Biham, Orr Dunkelman και Nathan Keller δημοσίευσαν μια related-key rectangle (boomerang) επίθεση στο KASUMI που μπορεί να σπάσει και τους 8 κύκλους γρηγορότερα από την εξαντλητική αναζήτηση. Η επίθεση απαιτεί 254,6 απλά κείμενα, κάθε ένα από τα οποία έχει κρυπτογραφηθεί κάτω από το ένα από τέσσερα σχετικά κλειδιά, και έχει μια χρονική πολυπλοκότητα ισοδύναμη με 276,1 κρυπτογραφήσεις KASUMI. Ενώ αυτό δεν είναι μια πρακτική επίθεση, ακυρώνει μερικές αποδείξεις για την ασφάλεια των 3GPP πρωτοκόλλων που είχαν στηριχθεί στη θεωρούμενη δύναμη του KASUMI.

Το 2006 οι Elad Barkan, Eli Biham και Nathan Keller κατέδειξε τις επιθέσεις ενάντια στα A5/1 και A5/2, οι οποίες επιτρέπουν στους επιτιθεμένους για να καταγράψουν τις τηλεφωνικές συνομιλίες του GSM και να τις αποκρυπτογραφήσουν είτε στον πραγματικό χρόνο, είτε σε οποιοδήποτε μετέπειτα χρόνο

3.5.3 Υποστήριξη των A5 Αλγορίθμων στα MS

Είναι υποχρεωτικό για τους A5/1, A5/3 και για το μη κρυπτογραφημένο τρόπο να εφαρμοστούν στους κινητούς σταθμούς. Είναι απαγορευμένο να εφαρμόσουν το A5/2 στους κινητούς σταθμούς. Κανένας άλλος A5 αλγόριθμος δεν θα υποστηριχθεί στους κινητούς σταθμούς.

3.6 Zh και Zn Interfaces Βασισμένα στο Diameter Πρωτόκολλο

Η αλλαγή αυτή έχει παρουσιαστεί στις προδιαγραφές του UMTS έκδοση 7. Η αλλαγή είναι στο “Technical Specification Group Core Network and Terminals; Generic

Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage (29019)".

3.6.1 Γενική Αρχιτεκτονική Αυθεντικοποίησης (Generic Authentication Architecture-GAA)

Δεδομένου ότι η ψηφιακή σύγκλιση γίνεται σιγά -σιγά μια πραγματικότητα, οι χρήστες των σύγχρονων κινητών τηλεφώνων χρησιμοποιούν όλο και περισσότερες υπηρεσίες στο διαδίκτυο, όπως διάφορα sites. Επίσης, οι πάροχοι έχουν αρχίσει να προσφέρουν έναν αυξανόμενο αριθμό νέων υπηρεσιών. Ο χρήστης, για παράδειγμα, μπορεί να διαβάσει το mail του από τη σχολική webmail υπηρεσία του στο διαδίκτυο και να κουβεντιάσει με τους φίλους του με τη χρησιμοποίηση μιας στιγμιαίας υπηρεσίας μηνύματος και παρουσίας (Instant Messaging and Presence) που του προσφέρθηκε από τον χειριστή του. Το κοινό για πολλές από αυτές τις νέες υπηρεσίες είναι ότι απαιτούν την αυθεντικοποίηση. Είναι σαφές ότι στις προαναφερθείσες περιπτώσεις ο χρήστης δεν επιθυμεί για καθέναν να είναι σε θέση να διαβάσει το ηλεκτρονικό ταχυδρομείο του ή να κουβεντιάσει με το όνομά του. Επίσης, ο φορέας παροχής υπηρεσιών πρέπει να ξέρει ποιος χρησιμοποιεί την υπηρεσία, τουλάχιστον για λόγους τιμολόγησης.

Μέχρι τώρα, ο χρήστης έπρεπε να έχει πιστοποιητικά για κάθε υπηρεσία που επρόκειτο να χρησιμοποιήσει. Είτε έπρεπε να τις χρησιμοποιήσει με το χέρι, π.χ. με το γράψιμο του ονόματος χρήστη και του κωδικού πρόσβασής του όταν προκαλείτε ή διαμορφώνοντας τους σε μια εφαρμογή πελατών, ή έπρεπε να μπουν σε μια έξυπνη κάρτα, όπως οι κάρτες subscriber identity module (SIM) στα κινητά τηλέφωνα. Η ύπαρξη διάφορων πιστοποιητικών είναι ένα πρόβλημα όχι μόνο επειδή είναι ενοχλητικό για το χρήστη να το διαχειριστεί, αλλά και επειδή δεν είναι άνετο για τους χρήστες να τα ελέγχουν, είναι ακριβό για τους χειριστές και άλλους φορείς παροχής υπηρεσιών και φυσικά απαιτεί προσπάθεια από τους χρήστες επίσης. Παραδείγματος χάριν, μια WWW-βασισμένη υπηρεσία βασισμένη σε κάποιον τρίτο φορέα να στείλει τα πιστοποιητικά μέσω του ηλεκτρονικού ταχυδρομείου στο χρήστη και να του ζητήσει να αλλάξει τον κωδικό πρόσβασης το συντομότερο δυνατόν. Αυτό, φυσικά, δεν είναι πολύ ασφαλές, και απαιτεί το χρήστη να επιλέξει έναν καλό κωδικό

πρόσβασης και επίσης για να τον θυμηθεί. Ένα παράδειγμα για τις δαπάνες του provisioning για τους χειριστές είναι η διανομή των καρτών SIM: πρέπει να κατασκευαστούν και να σταλούν στους πελάτες κάπως. Πρέπει επίσης να αντικατασταθούν όταν προκύπτουν οι νέες υπηρεσίες και απαιτούν το νέο είδος λειτουργίας.

Η γενική αρχιτεκτονική αυθεντικοποίησης (Generic Authentication Architecture, GAA) είναι μια λύση στην αυξανόμενη ανάγκη για την επικύρωση και βασική συμφωνία μεταξύ του πελάτη και των υπηρεσιών για το διαδίκτυο ή στο κυψελοειδές δίκτυο του πάροχου. Το GAA αντιμετωπίζει το πρόβλημα που ορίζεται ανωτέρω με τη χρησιμοποίηση του ήδη επεκταμένου και ευρέως χρησιμοποιημένου συστήματος αυθεντικοποίησης του GSM ως βάση για τα νέα πιστοποιητικά και για τους πελάτες και για τους κεντρικούς υπολογιστές. Η κύρια ιδέα είναι ότι το GAA είναι μια υπηρεσία αυθεντικοποίησης που παρέχεται από τον πάροχο που επιτρέπει στον πελάτη και την υπηρεσία για να επικυρώσει η μια την άλλη. Εντούτοις, το GAA δεν παρέχει μια Single Sign On service υπηρεσία, ακριβώς τα κοινά μυστικά για τα αμφότερα τα συμβαλλόμενα μέρη.

Σαν ένα από τα κύρια πλεονεκτήματα του GAA είναι η δυνατότητα να χρησιμοποιηθεί ένα υπάρχον σύστημα αυθεντικοποίησης, η 3G αυθεντικοποίηση και η συμφωνία κλειδιών (Authentication and Key Agreement, AKA), είναι μόνο φυσικό ότι αυτό το πλεονέκτημα επεκτείνεται για να υποστηρίξει επίσης τις 2G κάρτες SIM.

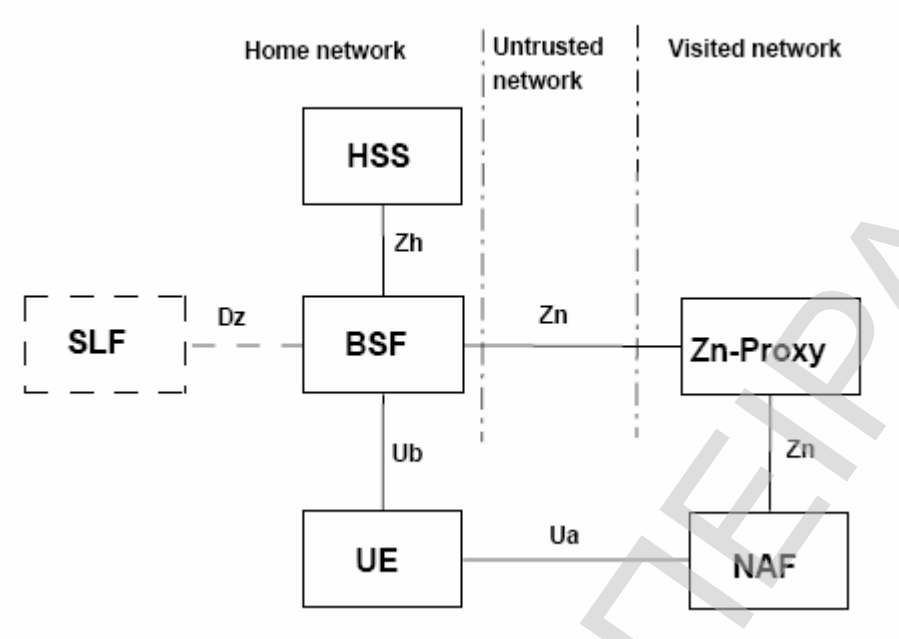
3.6.2 Επισκόπηση Συστήματος GAA

Υπάρχουν δύο κύριοι τρόποι για χρήση του GAA. Ο πρώτος είναι βασισμένος σε ένα κοινό μυστικό κλειδί μεταξύ του πελάτη και του κεντρικού υπολογιστή, και το δεύτερο στα δημόσια και ιδιωτικά ζευγάρια κλειδιά και τα ψηφιακά πιστοποιητικά. Στο κοινό μυστικό κλειδί, ο πελάτης και ο χειριστής πρώτα επικυρώνονται αμοιβαία με τη βοήθεια της 3G επικύρωσης και της βασικής συμφωνίας κλειδιών (AKA) και συμφωνούν σε session keys που μπορούν να χρησιμοποιηθούν μεταξύ του πελάτη και της υπηρεσίας που ο πελάτης θέλει να χρησιμοποιήσει. Αυτό καλείται bootstrapping. Μετά από αυτό οι υπηρεσίες μπορούν να προσκομίσουν τα κλειδιά συνόδου από το

χειριστή και μπορούν να χρησιμοποιηθούν σε κάποιο συγκεκριμένο πρωτόκολλο εφαρμογής μεταξύ του πελάτη και των υπηρεσιών.

Στη δεύτερη περίπτωση, το GAA χρησιμοποιείται για να επικυρώσει ένα αίτημα εγγραφής πιστοποιητικών από τον πελάτη. Πρώτα η διαδικασία έναρξης (bootstrapping) πραγματοποιείται όπως στην προηγούμενη περίπτωση. Μετά από αυτό ο πελάτης μπορεί να ζητήσει τα πιστοποιητικά από την υποδομή PKI του χειριστή, όπου η αυθεντικοποίηση γίνεται από τα κλειδιά συνόδου που λαμβάνονται με την ολοκλήρωση της διαδικασίας έναρξης. Αυτά τα πιστοποιητικά και τα αντίστοιχα βασικά ζευγάρια μπορούν έπειτα να χρησιμοποιηθούν για να παραγάγουν τις ψηφιακές υπογραφές ή για να αυθεντικοποίηθούν σε έναν κεντρικό υπολογιστή αντί της χρησιμοποίησης των κλειδιών συνόδου.

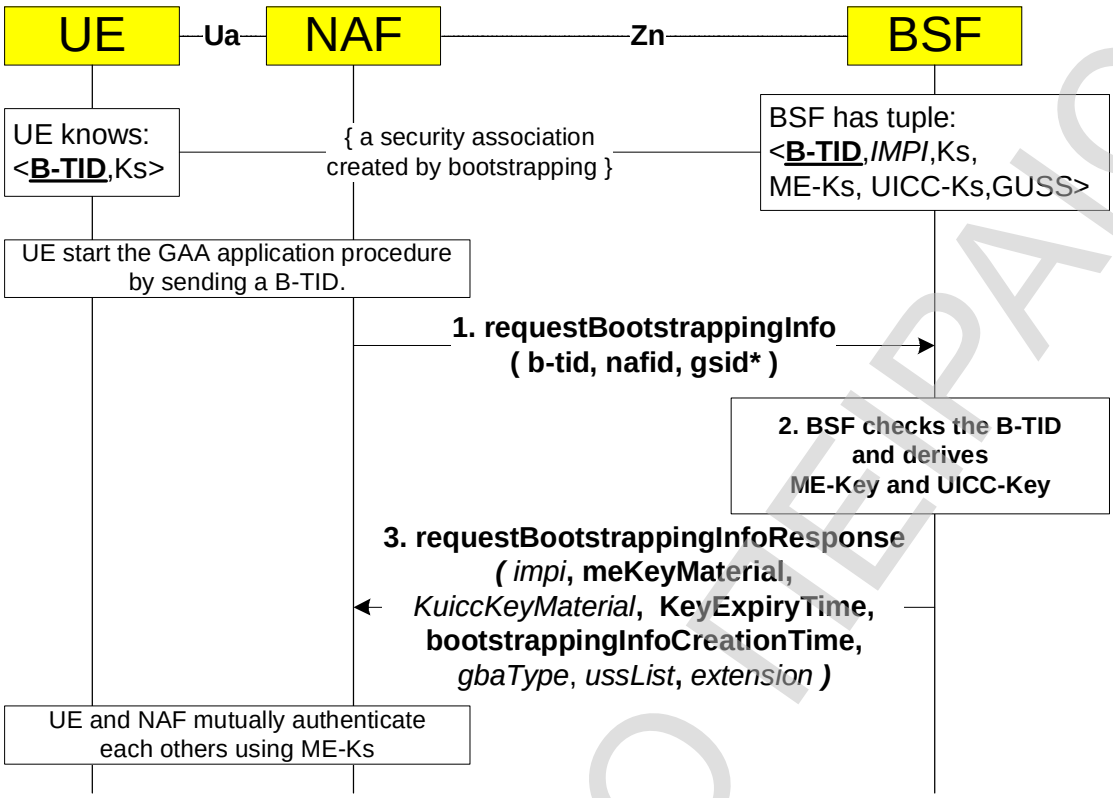
Το παρακάτω σχήμα παρουσιάζει τις οντότητες δικτύων GAA και τις διεπαφές μεταξύ τους. Ο εξοπλισμός (UE) των χρηστών είναι, παραδείγματος χάριν, το κινητό τηλέφωνο του χρήστη. Το UE και η λειτουργία κεντρικών υπολογιστών έναρξης (Bootstrapping Server Function -BSF) αμοιβαία επικυρώνονται πέρα από τη διεπαφή Ua, με τη χρησιμοποίηση του πρωτοκόλλου HTTP Digest AKA. Το UE επικοινωνεί επίσης με τα Network Application Functions (NAF), οι οποίες είναι οι κεντρικοί υπολογιστές εφαρμογής, πέρα από τη ua διεπαφή, η οποία μπορεί να χρησιμοποιήσει οποιοδήποτε συγκεκριμένο πρωτόκολλο εφαρμογής που είναι απαραίτητο. Το BSF ανακτά τα στοιχεία του συνδρομητή από τον Home Subscriber Server (HSS) πέρα από τη διεπαφή Zh, η οποία χρησιμοποιεί το πρωτόκολλο Diameter Base. Εάν υπάρχουν διάφορα HSSs στο δίκτυο, το BSF πρέπει πρώτα να υπολογίσει ποιο είναι σε χρήση. Αυτό μπορεί να γίνει με είτε τη διαμόρφωση ενός προκαθορισμένου HSS στο BSF, είτε με ένα query στο Subscriber Locator Function (SLF) πέρα από τη διεπαφή DZ. Τα NAFs ανακτούν τα κλειδιά συνόδου από το BSF πέρα από τη διεπαφή ZN, η οποία χρησιμοποιεί επίσης το Diameter Base πρωτόκολλο. Εάν το NFA δεν βρίσκεται στο εγχώριο δίκτυο, θα χρησιμοποιήσει ένα Zn-Proxy για να επικοινωνήσει με το BSF.



GAA Δικτυακές Οντότητες

3.6.3 Το Πρωτόκολλο Zn Μεταξύ NAF και BSF Βασισμένο σε Web Services

Οι διαδικασίες NAF και τα σχετικά με την BSF διεπαφή Web Services που είναι βασισμένη στο Zn interface αντί για Diameter messages, Web Services θα χρησιμοποιηθούν για να επικοινωνήσουν πέρα από τη διεπαφή Zn.



Web Services βασισμένα στο GAA

Τα βήματα της διαδικασίας εφαρμογής GAA είναι:

Βήμα 1

Το NAF θα στείλει ένα requestBootstrappingInfo μήνυμα στο BSF. Το schema του περιεχομένου μηνυμάτων δίνεται εδώ και θα είναι με το ίδιο format όπως είναι στο WSDL.

```
<xs:element name="requestBootstrappingInfo">
 <xs:complexType>
  <xs:sequence>
   <xs:element name="btid" type="xs:string"/>
   <xs:element name="nafid" type="xs:base64Binary"/>
   <xs:element name="gsid" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
   <xs:element name="extension" type="tExtension" minOccurs="0"/>
  </xs:sequence>
```

```
  </xs:complexType>
 </xs:element>
```

Το SOAP μήνυμα που θα σταλεί σε ένα BSF, δηλ., το URI του μηνύματος περιέχει τη διεύθυνση του BSF που εξάγεται από το B-TID. Στην περίπτωση όπου ο συνδρομητής έχει έρθει σε επαφή με το NAF που είναι σε ένα επισκεμμένο δίκτυο (visited network), οι NAF επαφές, το BSF του συνδρομητή μέσω ενός GBA-Proxy που βρίσκεται στο ίδιο δίκτυο με το NAF. Το τοπικό BSF και το GBA-Proxy μπορούν να συνδυαστούν. Το NAF δείχνει τις υπηρεσίες GAA για τις οποίες οι πληροφορίες ανακτώνται από τα στοιχεία «gsid». Το στοιχείο «btid» καθορίζει την προηγούμενη εκτέλεση διαδικασίας έναρξης (bootstrapping). Το NAF μπορεί να χρησιμοποιήσει ένα ή περισσότερα στοιχεία «extension» για να περιλάβει τα πρόσθετα στοιχεία στο αίτημα, αλλά το BSF μπορεί να αγνοήσει τα πρόσθετα στοιχεία.

Βήμα 2

Οι διαδικασίες για το βήμα 2 είναι οι ίδιες όπως ήταν προηγουμένως.

Βήμα 3

After that requestBootstrappingInfoResponse back to the NAF.

```
 <xs:element name="requestBootstrappingInfoResponse">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="impi" type="xs:string" minOccurs="0"/>
    <xs:element name="meKeyMaterial" type="xs:base64Binary"/>
    <xs:element name="uiccKeyMaterial" type="xs:base64Binary"
minOccurs="0"/>
    <xs:element name="keyExpiryTime" type="xs:dateTime"/>
    <xs:element name="bootstrappingInfoCreationTime" type="xs:dateTime"/>
    <xs:element name="gbaType" type="xs:string" minOccurs="0"/>
    <xs:element name="ussList" type="xs:string" minOccurs="0"/>
    <xs:element name="extension" type="tExtension" minOccurs="0"/>
   </xs:sequence>
```

```
  </xs:complexType>
</xs:element>
```

Το BSF μπορεί ή δεν μπορεί να στείλει το στοιχείο «impi» ανάλογα τη διαμόρφωσή του. Το υποχρεωτικό κοινό βασικό υλικό με το ΜΕ (Ks_NAF ή Ks_ext_NAF) στέλνεται στο στοιχείο "meKeyMaterial". Το κοινό βασικό υλικό με το UICC (Ks_int_NAF) στέλνεται προαιρετικά στο στοιχείο «uiccKeyMaterial» μόνο εάν η ετικέττα «uiccType» σε bsfInfo από το HSS τίθεται «GBA_U». Το στοιχείο «keyExpiryTime» περιέχει το χρόνο λήξης των πληροφοριών έναρξης στο BSF χορηγώντας τη διαμόρφωσή του. Εάν η διάρκειας ζωής ενός κλειδιού δίνεται στο tag «lifeTime» μέσα στο bsfInfo από το HSS η διαδικασία, θα χρησιμοποιηθεί αντί της κύριας διαμόρφωσης BSF όταν υπολογίζεται ο χρόνος λήξης. Το στοιχείο «bootstrappingInfoCreationTime» περιέχει το χρόνο δημιουργιών των bootstrapinfo, δηλ., το χρόνο δημιουργιών των πληροφοριών έναρξης (Bootstrapping) στο BSF. Το στοιχείο «ussList» περιέχει ένα αυτόνομο έγγραφο XML που περιέχει τις τοποθετήσεις ασφάλειας χρηστών. Το BSF θα δείξει τον τύπο χρησιμοποιημένης επικύρωσης στη διαδικασία έναρξης του NAF στο στοιχείο «gbaType», εάν εκτός από το 3G GBA ο τύπος έχει εκτελεστεί.

ΚΕΦΑΛΑΙΟ 4 :
ΣΥΜΠΕΡΑΣΜΑΤΑ

4. ΣΥΜΠΕΡΑΣΜΑΤΑ

Η πτυχιακή αυτή έχει σαν σκοπό να παρουσιάσει την εξέλιξη του UMTS από μια σκοπιά σχετική με την ασφάλεια. Περιλαμβάνει μια εισαγωγή στα 3G δίκτυα, στο UMTS και την ασφάλεια του και μια σύντομη αναφορά στο 4G. Επίσης γίνετε μια αναφορά στην υλοποίηση του UMTS δικτύου της Cosmote. Στο 2^{ο} κεφάλαιο υπάρχει μια ανασκόπηση της ασφάλειας του UMTS δικτύου στο επίπεδο του core network και του utran αλλά και του user equipment. Τέλος το 3^{ο} κεφάλαιο, περιέχει την εξέλιξη της ασφάλειας στο UMTS σύμφωνα με τα release που βγάζει το 3GPP και πιο συγκεκριμένα για τις αλλαγές στο user equipment αλλά και το utran. Η μεθοδολογία που ακολουθήθηκε ήταν η ακόλουθη. Αρχικά μέσω του web site του 3gpp κατέβηκαν όλα τα specs που υπήρχαν για τα release από 4 έως 8. Σε αυτά βρέθηκαν αυτά που αναφέρονταν στην ασφάλεια του UMTS και μετά βρέθηκαν σε αυτά οι διαφορές και συνεπώς η εξέλιξη στο τομέα της ασφάλειας του UMTS.

Το UMTS θα λέγαμε ότι ήταν μια λογική εξέλιξη στο τομέα των τηλεπικοινωνιών. Έρχεται να καλύψει την ανάγκη για νέες υπηρεσίες, πολυμεσικό περιεχόμενο και όλα αυτά σε λογικό κόστος και με υψηλές ταχύτητες. Επίσης πλέον δίνει τη δυνατότητα ο χρήστης να έχει πρόσβαση στο διαδίκτυο κάτι που βάζει σε νέο επίπεδο της τηλεπικοινωνίες και τις υπηρεσίες που προσφέρονται καθώς πλέον σε συνδυασμό με τις νέες συσκευές μπορούμε να έχουμε ένα μίνι υπολογιστή στην τσέπη μας. Όλα αυτά όμως δημιουργούν και νέες ανάγκες στον τομέα της ασφάλειας.

Η ασφάλεια στο UMTS στηρίζεται στο GSM με τη διατήρηση και βελτίωση των σημαντικών χαρακτηριστικών γνωρισμάτων ασφάλειάς του. Το UMTS έχει πολλά πλεονεκτήματα ασφάλειας έναντι του GSM, παρόλα αυτά το UMTS έχει επίσης και προβλήματα ασφάλειας από τη στιγμή που προσφέρει και υπηρεσίες διαδικτύου . Παραδείγματος χάριν όλα αυτά που θα μπορούσαν να συμβούν σε έναν σταθερό υπολογιστή που συνδέθηκε με το Διαδίκτυο θα μπορούσαν επίσης να συμβούν σε ένα τερματικό UMTS.

Κατά την διάρκεια της εξέλιξης του UMTS και των νέων release που έβγαλε το 3GPP, επιχειρήθηκε εκτός νέων υπηρεσιών και κάποιων αρχιτεκτονικών παρεμβάσεων να λυθούν και κάποια θέματα ασφαλείας . Καταρχάς έγιναν κάποιες

αλλαγές στην ασφάλεια του USIM Application Toolkit. Μπήκε η έννοια του Minimum Security Level αλλά και του USSD. Επίσης για να αντιμετωπιστεί η απάτη με τα SMS υποστηρίχτηκε το TCAP handshake μεταξύ των κινητών και του core network. Όσον αφορά τα MMS, αποφασίστηκε να ελέγχονται στους κόμβους του GSN στο PS domain. Επίσης όλοι οι mobile station είναι υποχρεωμένοι να επιλέγουν το αλγόριθμο κρυπτογράφησης KASUMI και όχι τον A5/2 όταν επικοινωνούν με τα base stations. Τέλος, οι διαδικασίες NAF(Network application functions) και τα σχετικά με την BSF διεπαφή που είναι βασισμένη στο Zn interface αντί για Diameter messages, πλέον θα χρησιμοποιηθούν Web Services για να επικοινωνήσουν πέρα από τη διεπαφή Zn. Αυτές είναι κάποιες από τις αλλαγές που είναι σχετικές με την ασφάλεια στο user equipment και το utran.

Το μέλλον της ασφάλεια του UMTS έχει αρκετές νέες προκλήσεις. Τα κινητά συστήματα θα πρέπει να προσαρμοστούν σε διάφορα νέα ραδιο-δίκτυα πρόσβασης όπως πχ των wireless δικτύων. Επίσης, από την πλευρά του χρήστη η έννοια του μονολιθικού τερματικού δεν υπάρχει πια. Τα κινητά τηλέφωνα πια επικοινωνούν με διάφορες άλλες συσκευές αλλά και μεταξύ τους. Ακόμα υπάρχει μια συνεχής ροή νέων υπηρεσιών οι οποίες πολλές φορές αλληλεπιδρούν με το διαδίκτυο. Όλα αυτά δημιουργούν νέες προκλήσεις στο τομέα της ασφάλειας. Ακόμα δεν θα πρέπει να ξεχνάμε πως παρά τα υψηλά στάνταρ στο τομέα ασφάλειας υπάρχουν ακόμα κάποια θέματα. Η αποστολή του IMSI σε απλό κείμενο όταν ο χρήστης μπαίνει στο δίκτυο για πρώτη φορά είναι ένα πρόβλημα. Εδώ η παρουσία μια τρίτης οντότητας (trusted third party) ίσως ήταν μια λύση. Επίσης υπάρχουν επιθέσεις όπως οι man-in-the-middle επιθέσεις και η παρουσία παραπλανητικών base stations. Τα διάφορα προβλήματα που προκύπτουν από την διασύνδεση του τερματικού με άλλα δίκτυα όπως internet ή Bluetooth (ύπαρξη λογισμικού που παγιδεύει το τηλέφωνο και επικοινωνεί με Bluetooth με τον υποκλοπέα) κάνουν θεωρώ αναγκαία την ύπαρξη πλέον και ενός anti virus για κινητά τηλέφωνα. Τέλος, καλή ιδέα θα ήταν η ύπαρξη ενός τύπου SSL. Ένα SSL το οποίο θα ήταν υπεύθυνο για την ασφάλεια των δεδομένων από το ένα τερματικό ως το άλλο, αλλά και θα προστάτευε από ωτακουστές, πλαστά μηνύματα και θα εγγυόταν την αυθεντικότητα της επικοινωνίας.

Η εξέλιξη του UMTS και των ασύρματων δικτύων ακούει στο όνομα 4G. Το 4G θα επιχειρήσει να ενώσει τα Wireless Local Area Networks που πλέον υπάρχουν παντού

με την 3G τεχνολογία. Ο σκοπός είναι να δημιουργηθούν δίκτυα που θα προσφέρουν ακόμα πιο πολλές υπηρεσίες και φυσικά σε πιο υψηλές ταχύτητες και όλα αυτά με ασφάλεια. Βέβαια θα πρέπει να λυθούν πολλά θέματα ασφαλείας καθώς το 4G είναι θα λέγαμε ένας συνδιασμός του 3G και του WLAN. Αυτό σημαίνει ότι εκτός από τα θετικά παίρνει και όλα τα προβλήματα ασφαλείας και των δύο συστημάτων. Το 4G θα επιχειρήσει να εφαρμόσει την φράση «Anytime, Anywhere», δηλαδή νέες υπηρεσίες οποιαδήποτε στιγμή και οπουδήποτε!

Κεφάλαιο 1

[1] *Security Architecture in UMTS Third Generation Cellular Networks,* Tomás Balderas-Contreras René A. Cumplido-Parra

[2] http://www.nttdocomo.com

[3] http://en.wikipedia.org/wiki/3G

[4] http://www.wisegeek.com/what-is-umts.htm

[5] *UMTS Security,* K. Boman, G. Horn, P. Howard, and V. Niemi

[6] http://www.umtsworld.com/technology/overview.htm

[7] *Security in third Generation Mobile Networks,* Christos Xenakis, Lazaros Merakos

[8] *Evaluation of UMTS security architecture and services,* Abdul Bais, Walter T. Penzhorn, Peter Palensky

[9] http://ntrg.cs.tcd.ie/

[10] http://www.tech-invite.com/Ti-ims-releases.html#fig4

[11] *Evolution of UMTS Architecture for Ser vice Development and Provisioning,* Sami Tabbane

[33] http://en.wikipedia.org/wiki/Radio_Network_Controller

[36] *Media gateway for mobile networks,* Magnus Fyro, Kai Heikkinen, Lars-Goran Petersen, and Patrik Wiss

Κεφάλαιο 2

[12] *Technical Specification Group Services and Systems Aspects; Network architecture, V5.9.0, Dec. 2002 ,* www.3gpp.org

[13] *Security in third Generation Mobile Networks,* Christos Xenakis

[14] *An Approach to full User Data Integrity Protection in UMTS Access Networks,* Ivo Pooters

Κεφάλαιο 3

[15] http://www.stouf.com

[16] *Technical Specification Group Core Network and Terminals; Security mechanisms for the (U)SIM application toolkit; Stage 2 (23048),* www.3gpp.org

[17] http://en.wikipedia.org/wiki/SIM_Application_Toolkit

[18] http://www.mobilein.com/ussd.htm

[19] http://www.truteq.com/tips/ussd/

[20] *Technical Specification Group Core Network and Terminals; Secured packet structure for (U)SIM Toolkit applications (31115),* www.3gpp.org

[21] *Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; MAP application layer security (33200),* www.3gpp.org

[22] http://www.telecomspace.com/ss7.html

[23] http://en.wikipedia.org/wiki/Signaling_System_7

[24] http://www.javvin.com/protocolTCAP.html

[25] http://en.wikipedia.org/wiki/Mobile_Application_Part

[26] http://en.wikipedia.org/wiki/Transaction_Capabilities_Application_Part

[27] *Technical Specification Group Services and System Aspects; 3G Security; Lawful interception architecture and functions. (33107),* www.3gpp.org

[28] http://www.ericsson.com/ericsson/corpinfo/publications/review

[29] http://www.it.kth.se/courses/2G1330/2G1330_Max_Loubser_MMS-20050731.pdf

[30]http://www.cdg.org/news/events/CDMASeminar/2003_Tech_Forum/EricssonSandberg.pdf

[31] *Technical Specification Group Services and system Aspects; Security related network functions (43020),* www.3gpp.org

[32] http://cryptodox.com/A5

[34] *Technical Specification Group Core Network and Terminals; Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage (29019),* www.3gpp.org

[35] *Generic Authentication Architecture,* Timo Olkkonen, Helsinki University of Technology