ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Διδακτικής Τεχνολογίας και Ψηφιακών Συστημάτων

Μελέτη και ανάλυση των προτύπων ασφαλείας στα δίκτυα 3ης γενιάς

Πέππας Κωνσταντίνος

Η εργασία υποβάλετε για την μερική κάλυψη των απαιτήσεων με στόχο την απόκτηση του μεταπτυχιακού διπλώματος σπουδών στη Διδακτική της Τεχνολογίας και Ψηφιακά Συστήματα του Πανεπιστημίου Πειραιώς

Εισαγωγή

Η τεχνολογία τα τελευταία χρόνια έχει πραγματοποιήσει αλματώδη εξέλιξη και αυτό είναι κάτι που βλέπουμε παντού γύρω μας. Πέρα από το γεγονός ότι τα πάντα γίνονται μικρότερα και γρηγορότερα, έχουν την τάση να γίνονται και ασύρματα. Τα κινητά τηλέφωνα γίνονται όχι μόνο μικρότερα αλλά και γρηγορότερα όσον αφορά τη δυνατότητα περιήγησης στο Internet. Χάρη στις ταχύτητες τις οποίες προσφέρουν οι τεχνολογίες HSCSD και GPRS, εξασφαλίζουν όχι μόνο την κάλυψη των βασικών απαιτήσεων για την πρόσβασή στο Internet αλλά και τη λήψη ήχων, εικόνων, εφαρμογών ή ακόμα και μικρών βίντεο σε ικανοποιητικές ταχύτητες. Επιπλέον το HSCSD και το GPRS μπορούν να χρησιμοποιηθούν και για τη γρήγορη πρόσβαση από ηλεκτρονικό υπολογιστή με χρήση του κινητού τηλεφώνου σαν μόντεμ, υποκαθιστώντας σε αρκετές περιπτώσεις ακόμα και την πρόσβαση μέσω σταθερής τηλεφωνικής γραμμής.

Πρόσφατα έχει ανακαλυφθεί άλλη μια μέθοδος πρόσβασης, ακόμα γρηγορότερη από το GPRS και η οποία παρέχει ταχύτητες μέχρι 384 Kbps. Ο λόγος για την τεχνολογία EDGE, η οποία όμως δεν έγινε ιδιαίτερα γνωστή ούτε υιοθετήθηκε από τα δίκτυα όλου του κόσμου. Ο λόγος ίσως είναι προφανής, καθώς μια νέα ακόμα γρηγορότερη τεχνολογία, η UMTS, είχε ήδη αρχίσει να εμφανίζεται, οπότε τα δίκτυα έδωσαν μεγαλύτερο βάρος σε αυτή, θεωρώντας περιττή τη χρήση του EDGE.

1.1 3G/UMTS

Ο όρος UMTS προέρχεται από τα αρχικά των λέξεων "Universal Mobile Telecommunications System" (Παγκόσμιο Σύστημα Κινητών Τηλεπικοινωνιών). Πρόκειται για την εξέλιξη σε σχέση με την χωρητικότητα, την ταχύτητα μετάδοσης των δεδομένων και την ύπαρξη νέων

υπηρεσιών, των κινητών δικτύων δεύτερης γενιάς. Σήμερα, περισσότερα από εξήντα 3G/UMTS δίκτυα που χρησιμοποιούν την WCDMA τεχνολογία λειτουργούν σε 25 χώρες. Για την οργάνωση του όλου εγχειρήματος έχει θεσπιστεί ειδικός μη κερδοσκοπικός οργανισμός με την ονομασία Third Generation Partnership Project (3GPP) του οποίου μέλημα είναι η παρακολούθηση και η καθοδήγηση των εξελίξεων στην συγκεκριμένη τεχνολογική περιοχή [3].

Ανάμεσα στα πλεονεκτήματα των UMTS δικτύων ξεχωρίζουμε τους αυξημένους ρυθμούς μετάδοσης των δεδομένων και την ταυτόχρονη υποστήριξη μεγαλύτερου όγκου δεδομένων και φωνής. Πιο συγκεκριμένα, το UMTS δίκτυο στην αρχική του φάση, θεωρητικά προσφέρει ρυθμούς μετάδοσης δεδομένων έως και 384 kbps σε περιπτώσεις όπου παρατηρείται αυξημένη κινητικότητα του χρήστη. Αντίθετα, όταν ο χρήστης παραμένει ακίνητος οι ρυθμοί μετάδοσης αυξάνουν κατά πολύ φθάνοντας την τιμή των 2 Mbps. [1]

Εκτιμάται ότι στο μέλλον θα υπάρξει περαιτέρω αύξηση των ρυθμών μετάδοσης δεδομένων. Ήδη, ο 3GPP έχει θέσει σαν standard δύο νέες τεχνολογίες. Πρόκειται για το High Speed Downlink Packet Access (HSDPA) και το High Speed Uplink Packet Access (HSUPA) αντίστοιχα. Οι συγκεκριμένες τεχνολογίες ουσιαστικά αποτελούν εξέλιξη του UMTS, αφού υπόσχονται ρυθμούς μετάδοσης των δεδομένων έως και 14,4 Mbps στο downlink και 5.8 Mbps στο uplink.

Αναλυτικά οι καινοτομίες που φέρνει το UMTS, κυρίως όσον αφορά εφαρμογές χρήστη είναι:

1) *Γρήγορη πρόσβαση στο Internet*: Τα 43 Kbps του HSCSD και του GPRS αν και καλύπτουν αρκετές απαιτήσεις για την ασύρματη πρόσβαση στο Internet, θα θεωρούνται πλέον αργά μπροστά στις εντυπωσιακές ταχύτητες που έχει να προσφέρει το UMTS. Με ρυθμούς μετάδοσης δεδομένων που ξεκινήσουν από τα 384 Kbps και σταδιακά με την επέκταση της κάλυψης και αναβάθμιση του εξοπλισμού των δικτύων θα φτάσουν τα 2 Mbps, θα υπάρχει πρόσβαση στο Internet από όπου και αν βρίσκεται ο χρήστης.

2) *Ταχύτερη αποστολή και λήψη MMS.* Αν μέχρι τώρα για να ολοκληρωθεί η αποστολή ενός MMS με εικόνες, video και ήχους απαιτούνταν 1-2 λεπτά, με το UMTS όλα αυτά θα γίνονται μέσα σε λίγα δευτερόλεπτα. Επιπλέον το UMTS θα επιτρέψει την αποστολή μηνυμάτων MMS με συνημμένα αρχεία μεγαλύτερου μεγέθους από ό,τι έχουμε συνηθίσει μέχρι

σήμερα. Για παράδειγμα η αποστολή ενός συνημμένου αρχείου 200 KB, που σήμερα με την υπάρχουσα τεχνολογία (MMS over GPRS) είναι αδύνατη ή στην καλύτερη περίπτωση χρειάζεται 4-5 λεπτά για να ολοκληρωθεί, με την υπηρεσία MMS μέσω UMTS η αποστολή θα διαρκεί λιγότερο από ένα λεπτό.

3) ***Streaming audio & video***: Πέρα από το download έτοιμων αρχείων ήχου και video, το UMTS επιτρέπει την παρακολούθηση ζωντανών προγραμμάτων μέσω Internet σε άριστη ποιότητα, χωρίς καθυστερήσεις και διακοπές. Η παρακολούθηση live αθλητικών μεταδόσεων ή η ακρόαση ραδιοφωνικών προγραμμάτων και νέων τραγουδιών μέσω Internet είναι μόνο μερικά παραδείγματα για αυτά που μπορεί να παρακολουθήσει ο χρήστης.

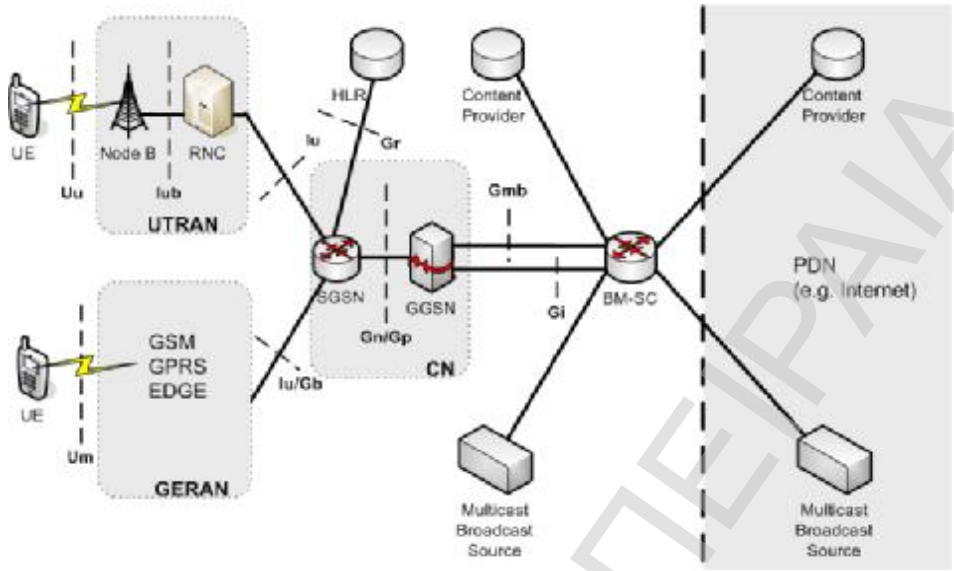
4) ***Video-conference***: Οι απλές τηλεφωνικές συνομιλίες με ήχο είναι κάτι ακόμα που αλλάζει ριζικά με την έλευση της νέας τεχνολογίας. Οι υψηλές ταχύτητες του UMTS επιτρέπουν όχι μόνο τη συνομιλία με ήχο αλλά τη δυνατότητα παρακολούθησης το του συνομιλητή σε πραγματικό χρόνο, σε συνδυασμό με τη χρήση της ενσωματωμένης κάμερας που διαθέτουν τα κινητά τηλέφωνα τρίτης γενιάς.

5) ***Online*** *αγορές και συναλλαγές*: Το UMTS φέρνει πραγματική επανάσταση και στον τρόπο με τον οποίο πραγματοποιούνται οι αγορές. Η κράτηση θέσεων για αεροπορικά δρομολόγια, η αγορά νέων προϊόντων ή η πληρωμή λογαριασμών θα είναι μόνο μερικά παραδείγματα από τις ευκολίες που θα φέρει στη ζωή του χρήστη, αφού όλα θα γίνονται μέσω ενός κινητού τηλεφώνου. Κάποιες από αυτές είναι ήδη σε εφαρμογή με το GPRS, ωστόσο με το UMTS όλα αυτά θα γίνονται ακόμα πιο άμεσα, γρήγορα και με μεγαλύτερη ασφάλεια.

6) *Υπηρεσίες κατά τοποθεσία*. Ας υποθέσουμε το ακόλουθο σενάριο: Ο χρήστης επισκέπτεται ένα άγνωστο μέρος για τις διακοπές του και επιθυμεί να μάθει ποια μέρη υπάρχουν για την διασκέδαση του. Το UMTS θα παρέχει έναν ενημερωμένο κατάλογο με σημεία διασκέδασης, αγορών αλλά και πρώτης ανάγκης που είναι προσβάσιμος ανα πάσα στιγμή στο κινητό τηλέφωνο. Συνεπώς ο χρήστης είτε αναζητεί μέρη για την ψυχαγωγία του, είτε βρίσκεται σε κατάσταση ανάγκης, το UMTS θα τον ενημερώσει για τα πλησιέστερα σημεία που θα τον εξυπηρετήσουν, ανάλογα με την περιοχή που βρίσκεται.

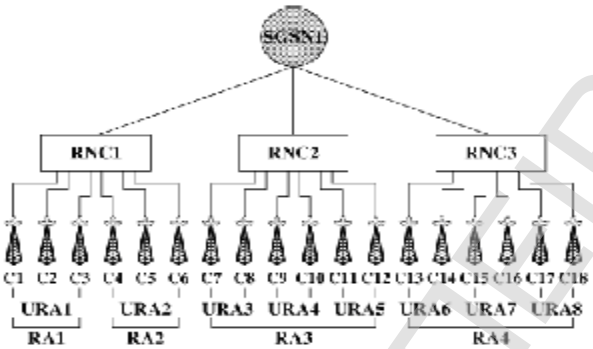
1.1.1 Αρχιτεκτονική UMTS

Στην συνέχεια παρουσιάζεται η αρχιτεκτονική ενός UMTS δικτύου καθώς και διάφορα άλλα σχετικά θέματα όπως η διαχείριση της κινητικότητας των χρηστών. Πιο συγκεκριμένα, ένα δίκτυο UTMS αποτελείται από δύο βασικές οντότητες: το **δίκτυο κορμού (CN - core network)** και το **δίκτυο επίγειας ασύρματης πρόσβασης (UTRAN - UMTS terrestrial radio-access network)** [2]. Το δίκτυο κορμού είναι υπεύθυνο για την δρομολόγηση των τηλεφωνημάτων καθώς και για τις συνδέσεις για μεταφορά δεδομένων με εξωτερικά δίκτυα. Αντίθετα, το UTRAN είναι υπεύθυνο για οτιδήποτε σχετίζεται με το ασύρματο μέρος του δικτύου. Το CN αποτελείται από δύο domain: α) circuit -switched (CS - μεταγωγή κυκλώματος), β) packet-switched (PS - μεταγωγή πακέτου). Το CS domain παρέχει πρόσβαση στο PSTN/ISDN , ενώ το PS domain παρέχει πρόσβαση στα IP δίκτυα. Στο εξής μας ενδιαφέρει το PS domain. Έτσι λοιπόν, το PS μέρος του UMTS δικτύου αποτελείται από δύο GPRS κόμβους υποστήριξης: τον gateway GPRS support node (GGSN) και τον serving GPRS support node (SGSN). Ο SGSN συνδέεται με τον SGSN μέσω της διεπαφής Gn και με το UTRAN μέσω της διεπαφής Iu. Το UTRAN αποτελείται από τον ελεγκτή ασύρματης πρόσβασης (RNC - radio network controller) και το Node B το οποίο αποτελεί την βάση που προσφέρει κάλυψη στο αντίστοιχο κελί. Το Node B συνδέεται με τον εξοπλισμό του χρήστη (user equipment - UE) μέσω της διεπαφής Uu (βασισμένο στην τεχνολογία W-CDMA) και με το RNC μέσω της διεπαφής Gi . Επιπλέον, υπάρχει και ένας άλλος κόμβος σχετιζόμενος με τις υπηρεσίες broadcast/multicast (BM-SC - broadcast/multicast service center), ο οποίος λειτουργεί σαν το σημείο εισόδου για την παραλαβή των δεδομένων για εσωτερικές πηγές. Τα παραπάνω παρουσιάζονται καλύτερα στο σχήμα που ακολουθεί:



Προτού ένας χρήστης είναι σε θέση να ανταλλάξει δεδομένα με ένα εξωτερικό PDN (Public Data Network), πρέπει να εγκαθιδρύσει μία εικονική σύνδεση με αυτό το PDN. Από την στιγμή που ο συγκεκριμένος κινητός χρήστης γίνει γνωστός στο δίκτυο, τα πακέτα μεταφέρονται μεταξύ αυτού και του δικτύου, βασισμένα στο packet data protocol (PDP), το οποίο αποτελεί το πρωτόκολλο του επιπέδου δικτύου του UMTS. Ένα στιγμιότυπο του PDP ονομάζεται PDP context και περιέχει όλες τις παραμέτρους που χαρακτηρίζουν την σύνδεση με το εξωτερικό δίκτυο όπως τις διευθύνσεις αποστολέα και παραλήπτη καθώς και την ποιότητα της υπηρεσίας. Ένα PDP context εγκαθιδρύεται για όλες τις εφαρμογές που κατευθύνονται προς ή προέρχονται από μία IP διεύθυνση. Μία ενεργοποίηση ενός PDP context ουσιαστικά αποτελεί μία διαδικασία αίτησης - απάντησης μεταξύ του κινητού χρήστη (UE) και του GGSN. Μία επιτυχής PDP context ενεργοποίηση οδηγεί στην δημιουργία δύο GPRS tunneling protocol (GTP) συνόδων για τον εκάστοτε χρήστη. Η πρώτη GTP σύνοδος δημιουργείται μεταξύ του GGSN και του SGSN πάνω από την διεπαφή Gn, ενώ η δεύτερη δημιουργείται μεταξύ του SGSN και του RNC πάνω από την διεπαφή Iu. Τα IP πακέτα τα οποία προορίζονται για μία εφαρμογή, χρησιμοποιώντας συγκεκριμένα GTP contexts, προσαρτώνται σε αυτά και μέσω του PDP μεταφέρονται στο αντίστοιχο SGSN. Το SGSN ανακτά τα IP πακέτα, ζητά το κατάλληλο PDP context βασισμένο στο UE και στο PDP και προωθεί τα πακέτα στο κατάλληλο RNC. Παράλληλα, το RNC διατηρεί έναν φορέα ασύρματης πρόσβασης (RAB - radio access bearer). Αντίστοιχα με τα PDP context, ένα RAB context επιτρέπει στο RNC να ανακτήσει την ταυτότητα του αποστολέα που έχει συσχετιστεί με ένα GTP. Αφού πλέον, το RNC έχει

ανακτήσει το πακέτο, το προωθεί στο κατάλληλο Node B. Τέλος, χρησιμοποιείται ένας tunnel endpoint identifier (TEID) στις διεπαφές Gn και Iu έτσι ώστε να μπορεί να αναγνωριστεί το τέλος του tunnel στον κόμβο που δέχεται τα πακέτα.



Στην συνέχεια, αναλύεται ο τρόπος με τον οποίο γίνεται η διαχείριση της κινητικότητας των UE (λεπτομέρειες παρουσιάζονται στο αντίστοιχο σχήμα). Έτσι λοιπόν, στο PS domain του UMTS, τα κελιά ομαδοποιούνται σε περιοχές δρομολόγησης (RAs - routing areas), ενώ τα κελιά σε μία περιοχή δρομολόγησης χωρίζονται περαιτέρω σε UTRAN registration areas (URAs). Επιπλέον, η διαχείριση της κινητικότητας (MM - mobility management) των κινητών χρηστών χαρακτηρίζεται από δύο μηχανές πεπερασμένων καταστάσεων: την μηχανή διαχείρισης της κινητικότητας (MM) και την radio resource control (RRC). Η μηχανή packet MM (PMM) του PS domain του UMTS εκτελείται μεταξύ του SGSN και του UE και είναι υπεύθυνη για τον έλεγχο στο επίπεδο του CN, ενώ η μηχανή RRC εκτελείται μεταξύ του UTRAN και του UE και είναι υπεύθυνη για τον σχετικό έλεγχο στο επίπεδο του UTRAN. Πιο συγκεκριμένα λοιπόν, αφότου ένα UE συνδεθεί στο PS domain, η μηχανή πεπερασμένων καταστάσεων PMM βρίσκεται σε μία από τις εξής δύο καταστάσεις: PMM idle ή PMM connected. Αντίστοιχα η μηχανή RRC μπορεί να βρίσκεται σε μία από τις εξής τρεις καταστάσεις: RRC idle, RRC cell - connected και RRC URA connected. Σημειώνεται ότι όταν δεν υπάρχει ροή δεδομένων μεταξύ του UE και του CN, το UE βρίσκεται στις καταστάσεις PMM idle και RRC idle αντίστοιχα. Στην περίπτωση αυτή το UTRAN δεν έχει καμία πληροφορία για το UE και το UE παρακολουθείται μόνο από το αντίστοιχο SGSN στο επίπεδο RA. Όταν ύστερα ξεκινήσει μία σύνδεση μεταξύ του UE και του SGSN, το UE μεταβαίνει στην κατάσταση PMM connected. Από την στιγμή που η σύνδεση στο PS λάβει χώρα, αυτόματα ξεκινά και μία RRC σύνδεση μεταξύ του UE και του αντίστοιχου RNC που το εξυπηρετεί. Σε αυτή την περίπτωση η RRC μηχανή για το συγκεκριμένο UE μεταβαίνει στην κατάσταση RRC cell - connected. Όταν κάτι

τέτοιο συμβεί, το SGSN παρακολουθεί το UE με ακρίβεια μέσω του αντίστοιχου RNC που εξυπηρετεί το UE. Το συγκεκριμένο RNC είναι υπεύθυνο να παρακολουθεί το κελί όπου το UE βρίσκεται κάθε στιγμή. Σημειώνεται ότι τα πακέτα μπορούν να ληφθούν από το UE μόνο όταν βρίσκεται σε αυτή την κατάσταση. Στην PMM connected/RRC cell - connected κατάσταση, αν το UE δεν έχει μεταδώσει/λάβει πακέτα για ένα συγκεκριμένο χρονικό διάστημα, η RRC μηχανή μεταβαίνει στην κατάσταση RRC URA connected. Σε αυτή την περίπτωση, η RCC σύνδεση διατηρείται ακόμη, ενώ το UE παρακολουθείται από το RNC που το εξυπηρετεί. Η συγκεκριμένη μετάβαση δεν επηρεάζει καθόλου την κατάσταση της PMM μηχανής για το συγκεκριμένο UE. Στην PMM connected / RRC URA connected κατάσταση, αν το UE μεταδώσει/λάβει ένα πακέτο, η RRC μηχανή μεταβαίνει πάλι στην κατάσταση RRC cell - connected. Αντίθετα, αν οι πόροι για τις συνδέσεις στο PS και RRC επίπεδο αποδεσμευτούν (για παράδειγμα όταν μία σύνοδος επικοινωνίας ολοκληρωθεί) ή αν κανένα πακέτο δεν έχει μεταδοθεί για ένα μεγάλο χρονικό διάστημα, η RRC μηχανή αρχικά μεταβαίνει στην RRC cell - connected κατάσταση και μετά στην RRC idle κατάσταση. Σε αυτή την περίπτωση, η PMM μηχανή αντίστοιχα μεταβαίνει στην PMM idle κατάσταση. Τέλος, όταν ένα UE δεν μπορεί να εντοπιστεί από το δίκτυο, η κατάστασή του χαρακτηρίζεται σαν PMM detached.

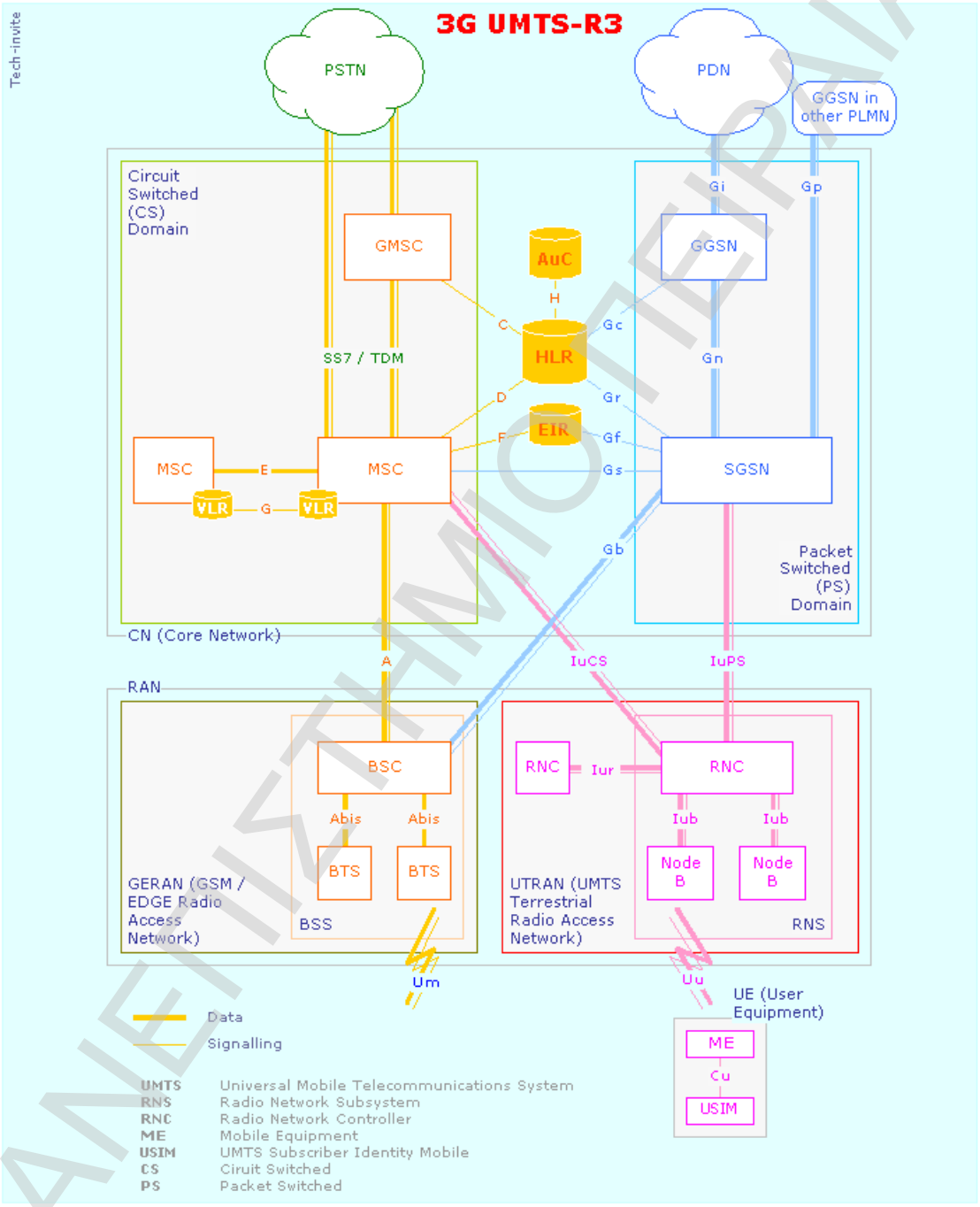
1.1.2 Αλλαγές στην αρχιτεκτονική UMTS και νέες υπηρεσίες

1.1.2.1 UMTS έκδοση 3

Η εισαγωγή των κινητών συστημάτων 3G με το UMTS έχει απαιτήσει την εγκατάσταση ενός εντελώς νέου ραδιο-υποσυστήματος, του UTRAN. Το κεντρικό δίκτυο του UMTS είναι βασισμένο στην ίδια τεχνολογία με το GSS, με πρόσθετους εξοπλισμούς, όπως είναι οι πύλες πολυμέσων (multimedia gateways, MG) για τη διασύνδεση των περιοχών δρομόλογησης πακέτων και με τις περιοχής μεταγωγής κυκλώματος.

Η πρώτη έκδοση του UMTS αυξάνει τις ταχύτητες μετάδοσης των δεδομένων έτσι ώστε υπηρεσίες πολυμέσων όπως η οπτική τηλεφωνία (visiophony), να μπορούν να παρασχεθούν στους συνδρομητές. Οι μεταβλητές ταχύτητες μετάδοσης στη ραδιο- διεπαφή είναι ένα άλλο πλεονέκτημα που προσφέρεται από το UMTS έναντι του 2 και του 2.5G. Με την έκδοση 3

(UMTS φάση 1) εισάγεται ένα νέο δίκτυο ραδιο-πρόσβασης το αποκαλούμενο UTRAN, που είναι βασισμένο στο W-CDMA αντί των TDMA/FDMA.



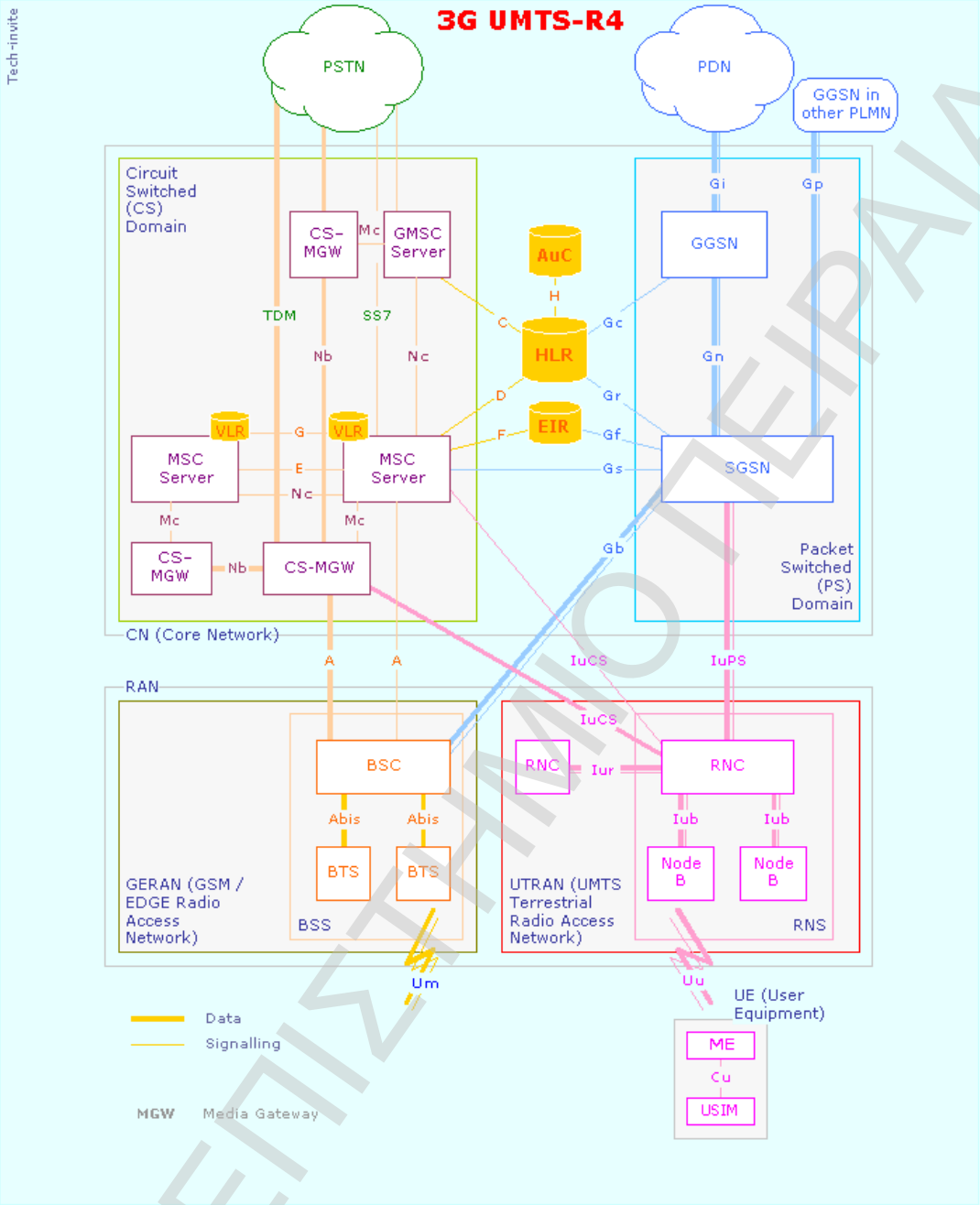
1.1.2.2 UMTS έκδοση 4

Στην ακόλουθη φάση εξέλιξης του UMTS, το τμήμα ραδιο-επικοινωνίας παραμένει σχεδόν αμετάβλητο. Στο επίπεδο κεντρικού δικτύου, το MSC (mobile switching centre) και το VLR (visitor location register) γίνονται διακομιστές MSC και MG. Οι διακομιστές MSC διαχειρίζονται τις επικοινωνίες και την κινητικότητα των χρηστών και τα MG είναι αρμόδια για τις λειτουργίες δρομολόγησης. Ο διακομιστής MSC μπορεί να διαχειριστεί πολλά MG, το οποίο επιτρέπει καλύτερο διαχωρισμό μεταξύ των λειτουργιών ελέγχου και των λειτουργιών δρομολόγησης. Αυτή η εξέλιξη επιτρέπει καλύτερο χωρισμό μεταξύ των λειτουργιών ελέγχου και επεξεργασίας στο δίκτυο. Επομένως διευκολύνει την εισαγωγή νέων χαρακτηριστικών γνωρισμάτων και συνεπώς νέες υπηρεσίες.

Με την έκδοση 4, η λειτουργικότητα του MSC είναι χωρισμένη σε δύο οντότητες:

- Τον διακομιστή MSC που παρέχει τις λειτουργίες έλεγχου

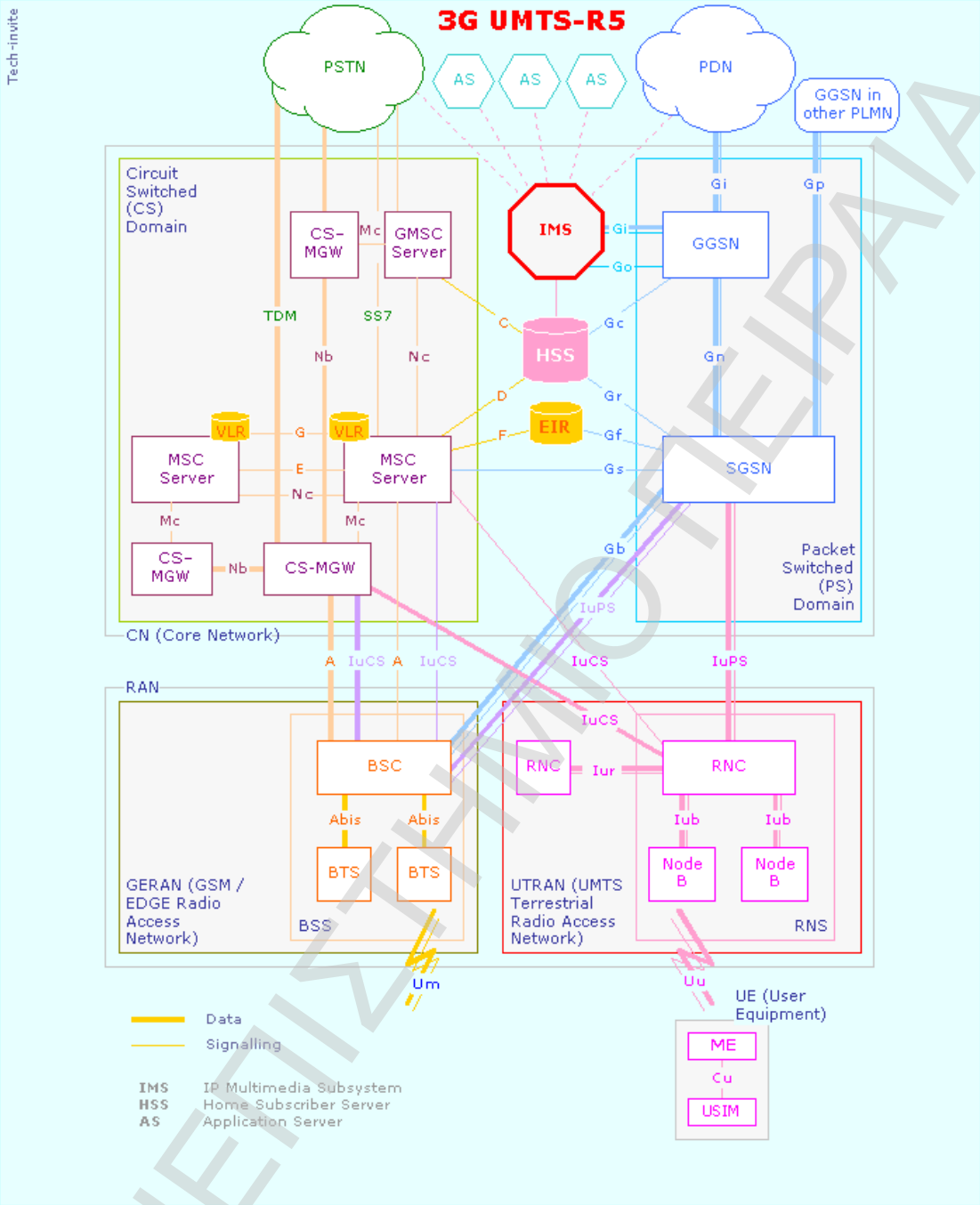
- Την MGW (Media Gateway) που παρέχει τις λειτουργίες bearer switching και εάν είναι απαραίτητο, τις συναρτήσεις μετατροπής μεταξύ των δύο διαφορετικών format. Ένας διακομιστής MSC μπορεί να ελέγχει πολλαπλά MGW.



1.1.2.3 UMTS έκδοση 5

Η έκδοση 5 των προδιαγραφών του UMTS είναι ένα κρίσιμο βήμα προς την ανάπτυξη και την εφαρμογή υπηρεσιών σε κινητό περιβάλλον. Η τεχνική HSDPA επιτρέπει μια σημαντική

αύξηση της ταχύτητας μετάδοσης καθώς είναι δυνατό να επιτευχθούν μερικά Mbits/δευτερόλεπτο (μέχρι 14) στο κανάλι downlink. Υπηρεσίες όπως βίντεο σε πραγματικό χρόνο, πρόσβαση στον Ιστό και σε FTP, κ.λπ. θα έχουν βελτιωμένες αποδόσεις ρυθμού δεδομένων. Το HSDPA επιτυγχάνεται κυρίως μέσα από τροποποιήσεις στο ραδιο-υποσύστημα. Στο επίπεδο δικτύου, η σημαντικότερη εξέλιξη που εισάγεται στο UMTS R5 είναι το υποσύστημα πολυμέσων IP, (IP Multimedia Subsystem, IMS), το οποίο παρέχει στους χειριστές τα μέσα που διευκολύνουν την εισαγωγή νέων υπηρεσιών και εφαρμογών πολυμέσων. Το IMS είναι ένα υποσύστημα που ελέγχει την παροχή υπηρεσιών μεταξύ των κεντρικών υπολογιστών και του κεντρικού δικτύου. Επιτρέπει την ενσωμάτωση των εφαρμογών πραγματικού χρόνου και των υπηρεσιών. Τέλος, το UMTS R5 εισάγει το IP στο ραδιο υποσύστημα (IP UTRAN) που γενικεύει τη χρήση του IP σε ολόκληρο το δίκτυο.



1.1.2.4 UMTS έκδοση 6

Η ραγδαία αύξηση των ασύρματων τοπικών δικτύων τα τελευταία χρόνια έχει παρακινήσει τους χειριστές για να ενσωματώσουν αυτήν την τεχνολογία στις δραστηριότητες και τα

επιχειρησιακά μοντέλα τους. Η χρήση αυτής της τεχνολογίας για την πρόσβαση στο Διαδίκτυο και σε υπηρεσίες και εφαρμογές που είναι βασισμένες στο IP, είναι ένα σημαντικό κίνητρο των χειριστών για το ενδιαφέρον τους για αυτήν την τεχνολογία που προέρχεται κυρίως από τον χώρο τον υπολογιστών. Η έκδοση 6 του UMTS θεωρεί τα WLAN ως τμήμα ολόκληρου του δικτύου. Μέσω ενός πλουσιότερου IMS (από την άποψη των χαρακτηριστικών γνωρισμάτων) θα είναι υπάρχει η δυνατότητα διαχείρισης της επικοινωνίας ανάμεσα σε σταθερά, κινητά και WLAN δίκτυα.

1.2 Mobile Security

Τα συστήματα κινητής τηλεφωνίας πρώτης γενιάς (1G) δεν παρείχαν σχεδόν κανένα χαρακτηριστικό ασφάλειας. Το σύστημα GSM (2G) σχεδιάστηκε έτσι ώστε να παρέχει ασφάλεια απέναντι σε φαινόμενα υποκλοπής φωνής και για να προστατεύσει από την κλωνοποίηση των κινητών ταυτοτήτων. Το GSM επιτρέπει στο χειριστή δικτύων να ελέγξει την ταυτότητα ενός χρήστη έτσι ώστε είναι ουσιαστικά αδύνατο για κάποιον να μεταμφιεστεί σε γνήσιο χρήστη. Η κρυπτογράφηση των δεδομένων των χρηστών και των πληροφοριών σηματοδότησης προστατεύει από την υποκλοπή τους. Στους χρήστες ορίζονται προσωρινές ταυτότητες. Αυτά τα χαρακτηριστικά γνωρίσματα αναφέρονται ως **επικύρωση**, **εμπιστευτικότητα** και **ανωνυμία**. Το νέο χαρακτηριστικό γνώρισμα της ασφάλειας GSM είναι η χρήση της SIM (Subscriber Identity Module), η οποία περιέχει όλα τα δεδομένα ταυτοποίησης και ασφάλειας για να μπορεί ο συνδρομητής να πραγματοποιήσει μια κλήση.

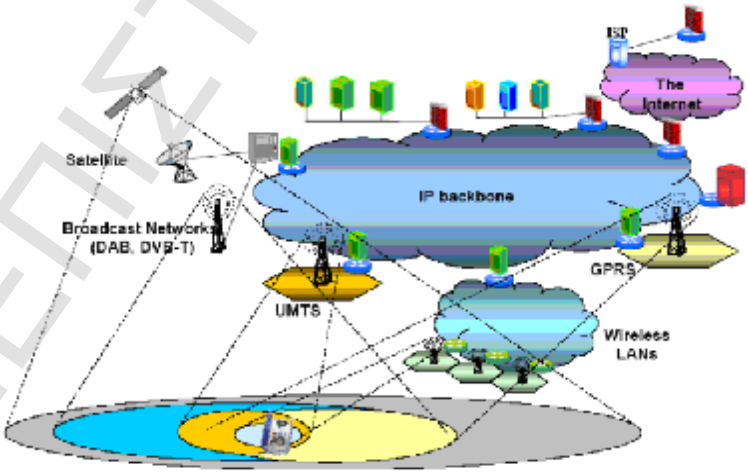
Η ασφάλεια UMTS στηρίζεται στην επιτυχία του GSM με τη διατήρηση (και ως ένα ορισμένο βαθμό τη βελτίωση) των σημαντικών και ισχυρών χαρακτηριστικών ασφάλειάς του. Αν και η ασφάλεια GSM είναι πολύ επιτυχής, ένας στόχος του σχεδιασμού ασφάλειας του UMTS ήταν να εξεταστούν οι πραγματικές και αντιληπτές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

- η νομική υποκλοπή δεν εξετάστηκε στην αρχική φάση σχεδιασμού.
- τα κλειδιά cipher και τα δεδομένα επικύρωσης διαβιβάζονται όπως είναι μεταξύ των δικτύων.

- ενεργές επιθέσεις που χρησιμοποιούν έναν «ψεύτικο σταθμό βάσης».
- δεν παρέχεται η ακεραιότητα των δεδομένων.
- η κρυπτογράφηση δεν επεκτείνεται αρκετά μακριά προς το κεντρικό δίκτυο και τα δεδομένα διαβιβάζονται χωρίς κρυπτογράφηση διαμέσου των ραδιο-συνδέσεων.ενεργές επιθέσεις που χρησιμοποιούν έναν «ψεύτικο σταθμό βάσης».
- τα συστήματα 2G δεν έχουν την ευελιξία να αναβαθμίσουν και να βελτιώσουν τη λειτουργία ασφάλειας με την πάροδο του χρόνου.

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

Η τεχνολογία εξελίσσεται διαρκώς και παρά το γεγονός ότι η τρίτη γενιά δεν είναι ακόμη σε πλήρη λειτουργία, η ακαδημαϊκή εξερεύνηση της 4G κινητής επικοινωνίας έχει ήδη ξεκινήσει. Καταρχήν η τρίτη γενιά ασφαλώς ήταν το βασικότερο βήμα για την επίτευξη των προσωπικών τηλεπικοινωνιών, αλλά ωστόσο δεν κατάφερε να τις κάνει πραγματικότητα.



Η τέταρτη γενιά θα προσεγγίσει περισσότερο τις προσωπικές επικοινωνίες παρέχοντας επικοινωνία οποιαδήποτε μορφής, σε κάθε χώρο και χρόνο, με οποιονδήποτε. Θα απαιτήσει επίσης καλή απόδοση επικοινωνίας, που θα αφορά κυρίως media παρά φωνή. Στις εφαρμογές τα τερματικά της τέταρτης γενιάς δε θα παρέχουν μόνο ομιλία ή εικόνα αλλά επιπλέον θα

προειδοποιεί και θα ενημερώνει το χρήστη. Τα τερματικά μπορεί ακόμα να γίνουν μέρος του ανθρώπινου σώματος, ενημερώνοντας το χρήστη για την πίεσή του, τη θερμοκρασία του κ.α.

Αναφορές

[1] http://www.umts-forum.org/

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

[3] http://www.3gpp.org/

Κεφάλαιο 2

Δίκτυα

2.1 Ασφάλεια σε κινητά δίκτυα τρίτης γενιάς (UMTS)

Για την προστασία ασφάλειας στα 3G-δίκτυα πρέπει να λάβουμε υπόψη μας αρκετούς παράγοντες , όπως είναι η ασύρματη πρόσβαση, η φορητότητα των τελικών χρηστών, οι απειλές ασφάλειας, το είδος πληροφοριών που θα πρέπει να προστατευτεί και η πολυπλοκότητα της δικτυακής αρχιτεκτονικής. Η ραδιο-μετάδοση είναι από τη φύση της πιο ευαίσθητη στην υποκλοπή δεδομένων και την απάτη σε σχέση με την ενσύρματη μεταφορά δεδομένων. Η φορητότητα των χρηστών και η καθολική πρόσβαση στο δίκτυο προκαλούν απειλές στην ασφάλεια. Οι διαφορετικοί τύποι δεδομένων, όπως τα δεδομένα των χρηστών, τα δεδομένα χρέωσης και τιμολόγησης, τα δεδομένα πληροφοριών των πελατών και τα δεδομένα διαχείρισης του δικτύου, που μεταβιβάζονται ή είναι μόνιμα στα κινητά δίκτυα, απαιτούν διαφορετικούς τύπους και επίπεδα προστασίας. Επιπλέον, οι σύνθετες τοπολογίες δικτύων και η ετερογένεια των χρησιμοποιούμενων τεχνολογιών, αυξάνουν τις προκλήσεις σε θέματα αξιοπιστίας.

Τα βασικά στοιχεία ασφάλειας που προέρχονται από το GSM είναι:

- Η πιστοποίηση των συνδρομητών

- Εμπιστευτικότητα της ταυτότητας συνδρομητών
- Το Subscriber Identity Module (SIM) να είναι αφαιρούμενο από το υλικό των τερματικών
- Κρυπτογράφηση της ραδιο-διεπαφής

Επιπρόσθετα γνωρίσματα ασφάλειας του UMTS:

- Ασφάλεια ενάντια στη χρήση ψεύτικων σταθμών βάσης, χρησιμοποιώντας αμοιβαία πιστοποίηση
- Κρυπτογράφηση που επεκτείνεται στη σύνδεση Node-B με RNC
- Τα δεδομένα ασφάλειας στο δίκτυο θα είναι προστατευμένα και στις αποθήκες δεδομένων και καθώς γίνονται οι μεταφορές των κλειδιών και των δεδομένων πιστοποίησης στο σύστημα.
- Μηχανισμός για αναβάθμιση στα χαρακτηριστικά γνωρίσματα ασφάλειας.

Η κυκλοφορία στο βασικό δίκτυο (core network) μεταξύ RNCs, των MSCs και άλλων δικτύων δεν κρυπτογραφείται και οι χειριστές μπορούν να εφαρμόσουν πολιτικές προστασίας για τις συνδέσεις μετάδοσης στο κεντρικό δίκτυο, αλλά αυτό δεν συμβαίνει συνήθως. Τα MSCs θα έχουν εκ σχεδιασμού ικανότητες νόμιμης υποκλοπής (lawful interception) και πρόσβασης στα αρχεία δεδομένων κλήσης (SDR), έτσι όλοι οι μεταγωγείς (switches) θα πρέπει να έχουν μέτρα ασφάλειας ενάντια στην παράνομη πρόσβαση.

Η προδιαγραφή UMTS έχει πέντε ομάδες χαρακτηριστικών γνωρισμάτων ασφάλειας:

- Ασφάλεια πρόσβασης στο δίκτυο: Αυτό το χαρακτηριστικό γνώρισμα επιτρέπει στους χρήστες να έχουν ασφαλή πρόσβαση στις υπηρεσίες που παρέχονται από το 3G δίκτυο. Αυτό το χαρακτηριστικό είναι αρμόδιο για την παροχή της εμπιστευτικότητας ταυτότητας, της πιστοποίησης των χρηστών, της εμπιστευτικότητας, της ακεραιότητας και της επικύρωσης του κινητού εξοπλισμού. Η εμπιστευτικότητα ταυτότητας χρηστών παρέχεται με τη χρησιμοποίηση μιας προσωρινής ταυτότητας αποκαλούμενη IMUI (International Mobile User Identity). Η πιστοποίηση επιτυγχάνεται χρησιμοποιώντας μια μέθοδο επαλήθευσης απάντησης χρησιμοποιώντας ένα μυστικό κλειδί. Η εμπιστευτικότητα παρέχεται με τη βοήθεια ενός μυστικού κλειδιού κρυπτογράφησης (CK) που ανταλλάσσεται ως τμήμα της διαδικασίας

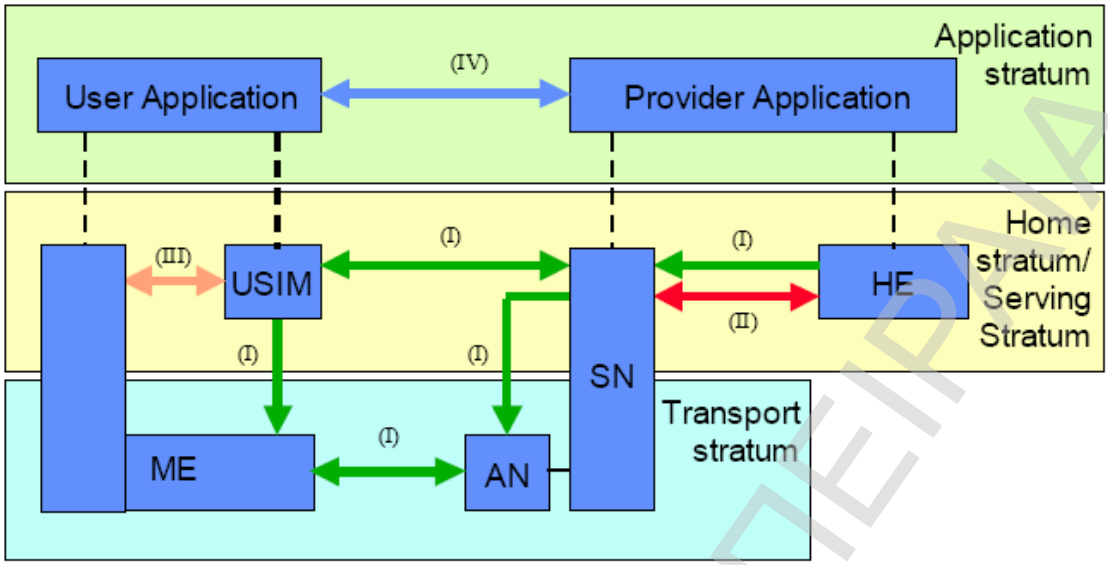
πιστοποίησης και συμφωνίας κλειδιού (Authentication and Key Agreement Process, AKA). Η ακεραιότητα παρέχεται χρησιμοποιώντας έναν αλγόριθμο ακεραιότητας και ένα κλειδί ακεραιότητας (IK). Η ταυτοποίηση του εξοπλισμού επιτυγχάνεται χρησιμοποιώντας το International Mobile Equipment Identifier (IMEI).

- Ασφάλεια περιοχής δικτύου: το σύνολο των γνωρισμάτων ασφάλειας που επιτρέπουν στους κόμβους στην περιοχή του παρόχου, να ανταλλάξουν ασφαλώς τα δεδομένα και που προστατεύουν από τις επιθέσεις στο δίκτυο γραμμών καλωδίου.

- Ασφάλεια περιοχής χρηστών: τα γνωρίσματα του USIM που επιτρέπουν μόνο σε εξουσιοδοτημένους χρήστες (δηλ, εκείνοι που ξέρουν τον προσωπικό αριθμό αναγνώρισης (PIN)) να έχουν πρόσβαση στο USIM και στο ΜΕ. Μερικά δεδομένα του USIM πρέπει να προστατευθούν από την πρόσβαση από το χρήστη.

- Η ασφάλεια περιοχής εφαρμογής περιλαμβάνει τους μηχανισμούς ασφάλειας για την πρόσβαση στα δεδομένα του προφίλ του χρήστη, ασφάλεια σε επίπεδο IP και τους μηχανισμούς για να παρέχει ασφαλείς ανταλλαγές μηνυμάτων μεταξύ του δικτύου και του USIM.

- Διαφάνεια και ρύθμιση της ασφάλειας: επιτρέπουν στους χρήστες να ενημερωθούν εάν ένα γνώρισμα ασφάλειας είναι σε λειτουργία και εάν η χρήση και η λειτουργία μιας υπηρεσίας είναι εξαρτώμενη από το γνώρισμα ασφάλειας.



Εικόνα 1. Επισκόπηση της αρχιτεκτονικής ασφαλείας

Η προδιαγραφή UMTS έχει τα ακόλουθα γνωρίσματα ασφάλειας της ταυτότητας χρηστών:

- Εμπιστευτικότητα ταυτότητας χρηστών: η ιδιότητα ότι η μόνιμη ταυτότητα χρήστη (IMSI) στον οποίο οι παραδίδονται υπηρεσίες, δεν μπορεί να υποκλαπεί στη ραδιο-σύνδεση (radio-link).

- Εμπιστευτικότητα θέσης χρηστών: η ιδιότητα ότι η παρουσία ή η άφιξη ενός χρήστη σε μια ορισμένη περιοχή δεν μπορεί να καθοριστεί με υποκλοπή στη ραδιο σύνδεση.

- Μη ανιχνευσιμότητα χρηστών: η ιδιότητα ότι ένας εισβολέας δεν μπορεί να συναγάγει εάν διαφορετικές υπηρεσίες παραδίδονται στον ίδιο χρήστη κάνοντας υποκλοπές στη ραδιο-σύνδεση.

Η κρυπτογράφηση/αποκρυπτογράφηση στην ασύρματη διεπαφή μετάδοσης πραγματοποιείται στο RNC στην πλευρά του δικτύου και στα κινητά τερματικά.

2.2 Ασφάλεια πρόσβασης Δικτύου

Η ασφάλεια πρόσβασης δικτύου είναι ένα βασικό συστατικό στην αρχιτεκτονική ασφαλείας του 3G. Αυτή η κατηγορία περιλαμβάνει το σύνολο μηχανισμών ασφάλειας που παρέχουν στους χρήστες ασφαλή πρόσβαση στις υπηρεσίες 3G, καθώς επίσης προστατεύουν από τις επιθέσεις στη ραδιο-σύνδεση. Αυτοί οι μηχανισμοί περιλαμβάνουν:

- εμπιστευτικότητα ταυτότητας χρηστών.
- πιστοποίηση και συμφωνία κλειδιών
- εμπιστευτικότητα δεδομένων
- προστασία ακεραιότητας των μηνυμάτων

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

2.2.1 Εμπιστευτικότητα ταυτότητας χρηστών

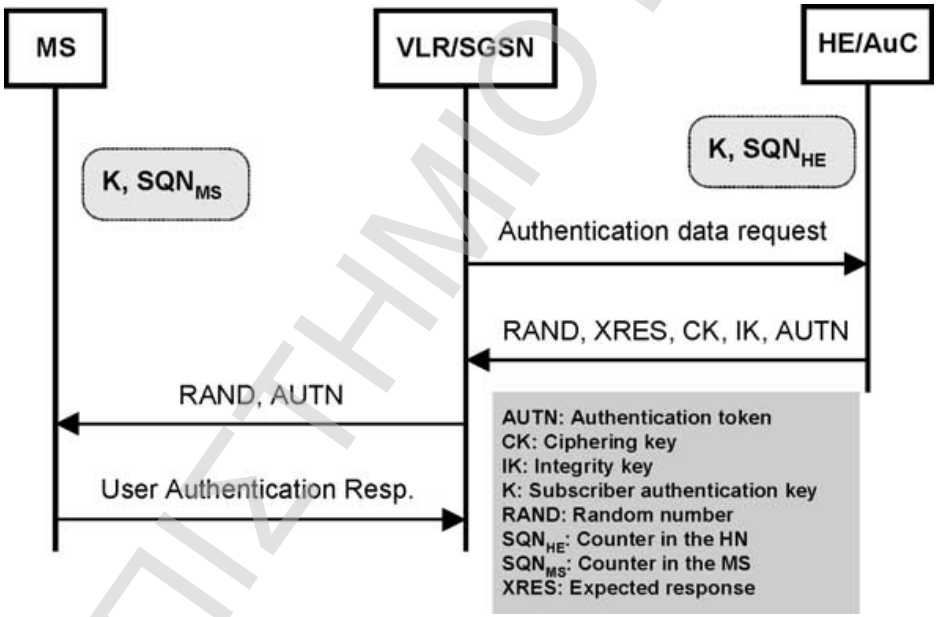
Η εμπιστευτικότητα ταυτότητας χρηστών επιτρέπει τον προσδιορισμό ενός χρήστη στη ραδιο-σύνδεση με τη βοήθεια μιας προσωρινής κινητής ταυτότητας συνδρομητών (Temporary Mobile Subscriber Identity, TMSI). Αυτό υπονοεί ότι η εμπιστευτικότητα της ταυτότητας χρηστών προστατεύεται σχεδόν πάντα από τους παθητικούς υποκλοπείς. Η αρχική εγγραφή είναι μια ειδική περίπτωση όπου μια προσωρινή ταυτότητα δεν μπορεί να χρησιμοποιηθεί, δεδομένου ότι το δίκτυο δεν ξέρει ακόμα τη μόνιμη ταυτότητα του χρήστη.

Η προσωρινή ταυτότητα μεταφέρεται στο χρήστη μόλις ενεργοποιηθεί η κρυπτογράφηση. Μια TMSI στην περιοχή CS ή μία P-TMSI στην περιοχή PS έχει τοπική σημασία μόνο στην περιοχή θέσης ή την περιοχή δρομολόγησης, στις οποίες ο χρήστης εγγράφεται. Η σχέση μεταξύ των μόνιμων και προσωρινών ταυτοτήτων χρηστών αποθηκεύεται στο Visited Location Register ή στο Serving GPRS Support Node (VLR/SGSN). Εάν ο κινητός χρήστης φθάνει σε μια νέα περιοχή, τότε η σχέση μεταξύ της μόνιμης και προσωρινής ταυτότητας μπορεί να προσκομιστεί από την παλαιά περιοχή θέσης ή δρομολόγησης. Εάν η διεύθυνση της παλαιάς περιοχής δεν είναι γνωστή ή η σύνδεση δεν μπορεί να δημιουργηθεί, η μόνιμη ταυτότητα πρέπει να ζητηθεί από τον κινητό χρήστη.

Για να αποφευγχει η ανιχνευσιμότητα χρηστών, που μπορεί να οδηγήσει στο συμβιβασμό της εμπιστευτικότητας ταυτότητας χρηστών καθώς επίσης και στην καταγραφή θέσης των χρηστών, ο χρήστης δεν πρέπει να ταυτοποιηθεί για μια μεγάλη περίοδο με τη βοήθεια της ίδιας προσωρινής ταυτότητας. Επιπλέον, οποιαδήποτε μηνύματα ή δεδομένα χρηστών όπου μπορούν να αποκαλύψουν την ταυτότητα του χρήστη, κρυπτογραφούνται στη ραδιο- σύνδεση.

2.2.2 Πιστοποίηση και συμφωνία κλειδιού

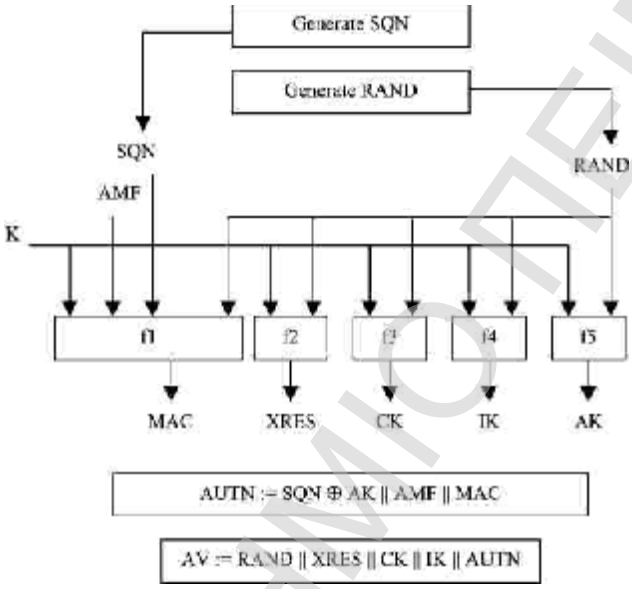
Η πιστοποίηση και η συμφωνία κλειδιού επιτυγχάνει την αμοιβαία πιστοποίηση μεταξύ του κινητού χρήστη και του SN που γνωρίζει ένα μυστικό κλειδί K.



Εικόνα 2. Πιστοποίηση και συμφωνία κλειδιού

Η μέθοδος πιστοποίησης αποτελείται από ένα πρωτόκολλο πρόκλησης/απάντησης και επιλέχτηκε με τέτοιο τρόπο ώστε να επιτευχθεί η μέγιστη συμβατότητα με την αρχιτεκτονική ασφάλειας GSM/GPRS που διευκολύνει τη μετάβαση από το GSM GPRS στο UMTS[1]. Επιπλέον, το USIM και το HE κρατάνε τους μετρητές SQNms και SQNhe αντίστοιχα, για να υποστηρίξουν την πιστοποίηση δικτύων. Ο αριθμός ακολουθίας SQNhe είναι ατομικός μετρητής για κάθε χρήστη, ενώ το SQNms υποδηλώνει τον υψηλότερο αριθμό ακολουθίας που έχει δεχτεί το USIM.

Με την παραλαβή ενός αιτήματος από το VLR/SGSN, το κέντρο επικύρωσης (HE/AuC) προωθεί μια διαταγμένη σειρά διανυσμάτων επικύρωσης (AV) στο VLR/SGSN. Κάθε AV, που χρησιμοποιείται στην επικύρωση και τη διαδικασία συμφωνίας κλειδιού μεταξύ του VLR/SGSN και του USIM, αποτελείται από έναν τυχαίο αριθμό RAND, μια αναμενόμενη απάντηση XRES, ένα κλειδί κρυπτογράφησης CK, ένα κλειδί ακεραιότητας IK, και ένα σύμβολο AUTN.



Εικόνα 3. Δημιουργία των διανυσμάτων πιστοποίησης

Το HE/AuC αρχίζει με την παραγωγή ενός νέου αριθμού ακολουθίας SQN, ο οποίος αποδεικνύει στο χρήστη ότι το παραγμένο AV δεν έχει χρησιμοποιηθεί ξανά. Κατόπιν, χρησιμοποιώντας το μυστικό κλειδί K υπολογίζει:

- Τον Κωδικό Πιστοποίησης Μηνύματος (Message Authentication Code),

MAC = f1k (SQN|| RAND ||AMF), όπου f1 είναι η συνάρτηση πιστοποίησης μηνυμάτων. Το AMF (Authentication and key Management Field) χρησιμοποιείται για να τελειοποιήσει την απόδοση ή να φέρει ένα νέο κλειδί πιστοποίησης που αποθηκεύεται στο USIM.

- Την αναμενόμενη απάντηση XRES = f2k(RAND) όπου το f2 είναι μια συνάρτηση επικύρωσης μηνυμάτων.
- Το κλειδί κρυπτογράφησης CK = f3k(RAND)
- Το κλειδί ακεραιότητας IK = f4k(RAND) και

- Το κλειδί ανωνυμίας (Anonymity Key) AK = f5k(RAND)

όπου f3, f4 και f5 είναι συναρτήσεις παραγωγής κλειδιών. Τέλος το HE/AuC κατασκευάζει το σύμβολο AUTN.

Πρέπει να σημειωθεί ότι η επικύρωση και οι συναρτήσεις παραγωγής κλειδιού f1, f2, f3, f4 και f5 και ο επακόλουθος υπολογισμός του AV, βασίζονται στην μονόδρομη ιδιότητα. Αυτό σημαίνει ότι εάν το αποτέλεσμα των συναρτήσεων είναι γνωστό, δεν υπάρχει κανένας αποδοτικός αλγόριθμος για να συναγάγει την είσοδο στην συνάρτηση που θα παρήγαγε το συγκεκριμένο αποτέλεσμα της συνάρτησης. Αν και οι συναρτήσεις f1-f5 είναι βασισμένες στον ίδιο βασικό αλγόριθμο, διαφέρουν μεταξύ τους με έναν θεμελιώδη τρόπο προκειμένου να είναι αδύνατον να συναχθεί οποιαδήποτε πληροφορία για το αποτέλεσμα μιας συνάρτησης από τα αποτελέσματα των άλλων συναρτήσεων. Δεδομένου ότι χρησιμοποιούνται στο AuC και στο USIM, το οποίο ελέγχεται από έναν χειριστή, η επιλογή των αλγορίθμων (f1 - f5) γίνεται από τον χειριστή. Εντούτοις, έχει προταθεί ένα σύνολο αλγορίθμων αποκαλούμενο MILENAGE.

Όταν το VLR/SGSN αρχικοποιεί μια διαδικασία επικύρωσης και μια διαδικασία συμφωνίας κλειδιού, επιλέγει το επόμενο AV από τη διαταγμένη σειρά και διαβιβάζει τις παραμέτρους RAND και AUTN στο χρήστη. Το USIM, που χρησιμοποιεί το μυστικό κλειδί K, υπολογίζει το AK, AK = f5k(RAND) και ανακτά το SQN. Κατόπιν, υπολογίζει το XMAC = f1k (SQN||AKPH||AMF) και ελέγχει εάν το λαμβανόμενο AUTN και οι ανακτημένες τιμές SQN παρήχθησαν πράγματι από το AuC.

Σε αυτή την περίπτωση, το USIM υπολογίζει το RES = f2k(RAND) και ειδοποιεί τον κινητό σταθμό (MS) για να στείλει πίσω μια απάντηση πιστοποίησης χρηστών. Κατόπιν το USIM υπολογίζει το CK = f3k (RAND) και το IK =f4k(RAND).

Το VLR/SGSN συγκρίνει το λαμβανόμενο RES με τον πεδίο XRES του AV. Εάν ταιριάζουν θεωρεί ότι η πιστοποίηση και η συμφωνία κλειδιών έχουν ολοκληρωθεί επιτυχώς. Τέλος το USIM και το VLR/SGSN μεταβιβάζουν τα καθιερωμένα κλειδιά κρυπτογράφησης και προστασίας ακεραιότητας (CK και IK) στον κινητό εξοπλισμό και στο Radio Network Controller (RNC) που εφαρμόζουν συναρτήσεις ακεραιότητας και κρυπτογράφησης.

2.2.3 Εμπιστευτικότητα δεδομένων

Μόλις επικυρώσουν ο χρήστης και το δίκτυο ο ένας τον άλλον, μπορούν να αρχίσουν την ασφαλή επικοινωνία μεταξύ τους. Όπως περιγράψαμε ένα κλειδί κρυπτογράφησης διαμοιράζεται μεταξύ του κεντρικού δικτύου και του τερματικού μετά από μια επιτυχής διαδικασία πιστοποίησης. Τα δεδομένα που στέλνονται ασύρματα μέσω της ραδιο-σύνδεσης υπόκεινται σε κρυπτογράφηση χρησιμοποιώντας τη συνάρτηση f8: Η διαδικασία κρυπτογράφησης/αποκρυπτογράφησης πραγματοποιείται στο MS και στο RNC από την πλευρά του δικτύου. Η f8 είναι ένας συμμετρικός σύγχρονος αλγόριθμος κρυπτογράφησης που χρησιμοποιείται για να κρυπτογραφήσει πλαίσια (frames) μεταβλητού μήκους. Η βασική είσοδος στην f8 είναι ένα μυστικό κλειδί κρυπτογράφησης CK μήκους 128-bit. Επιπρόσθετες είσοδοι, που χρησιμοποιούνται για να βεβαιώσουν ότι δύο πλαίσια κρυπτογραφούνται με διαφορετικά keystreams, είναι η τιμή COUNT μήκους 32-bit, η τιμή BEARER μήκους 5-bit και η τιμή DIRECTION μήκους 1-bit. Το αποτέλεσμα είναι μια αλληλουχία απο bits (το ονομαζόμενο keystream) ίδιου μήκους με το πλαίσιο. Το πλαίσιο κρυπτογραφείται κάνοντας XOR τα δεδομένα με το keystream. Στο UMTS R99, η f8 βασίζεται στον αλγόριθμο Kasumi.

Ο αλγόριθμος KASUMI [2] είναι block cipher που λειτουργεί με 64-bit block χρησιμοποιώντας ένα κλειδί μήκους 128-bit. Είναι βασισμένος σε μια δομή Feistel με 8-γύρους (ο 3DES έχει μια δομή Feistel με 48-γύρους). Η συνάρτηση f9 στο πρωτόκολλο ασφάλειας UMTS είναι μια συνάρτηση ακεραιότητας βασισμένη στον KASUMI. Παράγει ένα MAC για ένα μήνυμα με τη χρήση του KASUMI σε τρόπο CBC λειτουργίας. Εάν ένα μήνυμα αποτελείται από q n-bit blocks D1, D2… Dq, και Ek (X) είναι η κρυπτογράφηση του μπλοκ X που χρησιμοποιεί το κλειδί K, τότε η συνάρτηση f9 μπορεί να περιγραφεί ως εξής:

1) $H1 = Ek(D1)$,

2) $Hi = Ek(Di \oplus Hi-1)$

3) $MAC = Ek'(H1 \oplus H2 \oplus \ldots \oplus Hq)$.

Δεδομένου ότι ένα μπλοκ μεγέθους 64-bit είναι μάλλον μικρό για αυτήν την εφαρμογή, η f9 έχει μια πρόσθετη σύζευξη και χρησιμοποιεί δύο κλειδιά, K και K', για να είναι λιγότερο τρωτή στις επιθέσεις internal collision και τις επιθέσεις exor forgery.

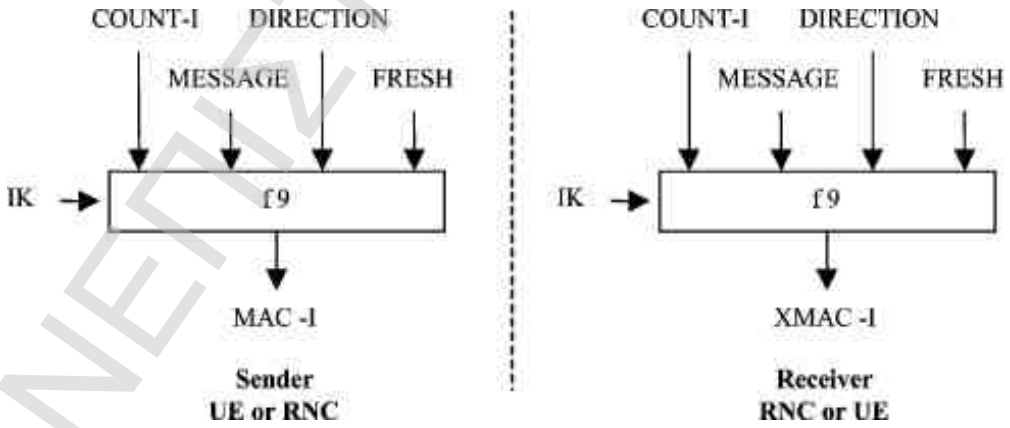
Οι εσωτερικές συγκρούσεις που προκαλούνται από μια επίθεση birthday θεωρούνται ανέφικτες χρησιμοποιώντας εσωτερική κατάσταση των 128-bit. Επιπλέον, αυτή η σύζευξη σε σχέση με ένα παραγόμενο δεύτερο κλειδί αποτρέπει μια επίθεση exor forgery. Ο KASUMI λειτουργεί με μέγεθος κλειδιού των 128-bit, τα οποία είναι αρκετά για τα επόμενα χρόνια για να

αποτρέψουν επιτυχείς επιθέσεις εξαντλητικής αναζήτησης κλειδιού. Δυστυχώς, η f9 δεν επιτρέπει μεταβλητή παράμετρο αποκοπής. Το εξηντατετράμπιτο αποτέλεσμα έχει σταθερή αποκοπή σε MAC των 32 bits. Αυτή η αποκοπή σε μερικές περιπτώσεις κάνει περισσότερο εφικτή μία τυχαία επίθεση.

2.2.4 Προστασία ακεραιότητας των μηνυμάτων σηματοδότησης

Μόλις δημιουργηθεί ένα κλειδί ακεραιότητας, ως τμήμα ενός πρωτοκόλλου επικύρωσης και μόλις είναι γνωστοί οι διαθέσιμοι αλγόριθμοι προστασίας ακεραιότητας στο MS, το δίκτυο μπορεί να αρχίσει την προστασία ακεραιότητας. Η προστασία ακεραιότητας εφαρμόζεται στον κινητό εξοπλισμό (ME) στην πλευρά χρηστών και στο RNC στην πλευρά του δικτύου. Μια συνάρτηση MAC εφαρμόζεται σε κάθε μεμονωμένο μήνυμα σηματοδοσίας (signalling) στο επίπεδο RRC της στοίβας πρωτοκόλλου UTRAN.

Μετά από την καθιέρωση σύνδεσης RRC τα περισσότερα από τα επόμενα μηνύματα σηματοδοσίας RRC προστατεύονται ως προς την ακεραιότητα τους. Αυτό περιλαμβάνει τα ίδια τα μηνύματα σηματοδοσίας RRC, συν τα αποκαλούμενα μηνύματα άμεσης μεταφοράς RRC. Η προστασία των μηνυμάτων άμεσης μεταφοράς συνεπάγεται την προστασία στη διαχείριση κινητικότητας, στον έλεγχο κλήσης και στη διαχείριση συνόδου.



Εικόνα 4. **Χρήση της συνάρτησης ακεραιότητας** f9 **για την πιστοποίηση ενός μηνύματος σηματοδότησης** RRC

Οι παράμετροι εισόδου για τον αλγόριθμο είναι:

- Το κλειδί ακεραιότητας IK, που έχει μήκος 128 bit

- Ένας αριθμός ακεραιότητας COUNT-I και μια τυχαία τιμή FRESH που παράγεται από το RNC. Οι τιμές COUNT-I καιFRESH έχουν μήκος 32 bit η καθεμία.

Βασιζόμενος σε αυτές τις παραμέτρους εισόδου, ο αποστολέας υπολογίζει το MAC των 32 bit για την ακεραιότητα των δεδομένων (MAC-I) χρησιμοποιώντας την f9.

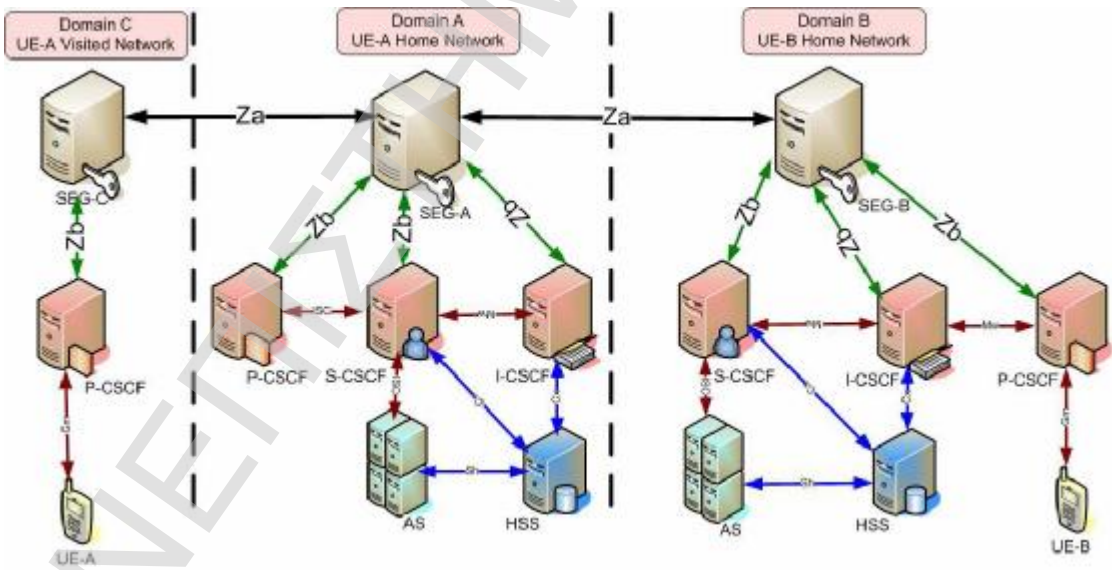
Το MAC-I επισυνάπτεται στο μήνυμα RRC όταν στέλνεται μέσω της ραδιο-σύνδεσης. Ο δέκτης υπολογίζει το αναμενόμενο MAC-I (XMAC-I) στο μήνυμα που έχει ληφθεί, με τον ίδιο τρόπο που ο αποστολέας υπολόγισε το MAC-I στο μήνυμα που έστειλε και ελέγχει την ακεραιότητα δεδομένων του μηνύματος συγκρίνοντας το με το λαμβανόμενο MAC-I. Το γνώρισμα ακεραιότητας παρέχει επίσης την επικύρωση προέλευσης δεδομένων έτσι ώστε ο δέκτης ενός μηνύματος σηματοδοσίας να μπορεί να επιβεβαιώσει την ταυτότητα του αποστολέα. Αυτό επιτρέπει σε έναν χειριστή να μην τρέξει την πλήρη διαδικασία επικύρωσης και το πρωτόκολλο συμφωνίας κλειδιού κάθε φορά που δημιουργείται μια σύνδεση.

2.3 Ασφάλεια περιοχής δικτύου

Η περιοχή δικτύου (network domain) είναι ένα δίκτυο που ελέγχεται από την ενιαία αρχή διαχειριστών για να εφαρμόσει 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 της περιοχής εφαρμόζεται στα σύνορα του δικτύου του χειριστή (operator) και προστατεύεται από πύλες ασφάλειας (Security Gateways, SEGs). Το NDS/IP χρησιμοποιείται για να προστατεύσει το κεντρικό δίκτυο IMS και την κυκλοφορία μεταξύ των visited και των home δικτύων. Η θεμελιώδης ιδέα της αρχιτεκτονικής NDS/IP είναι να παρασχεθεί ασφάλεια hop-by-hop που βοηθά στην διατήρηση χωριστών πολιτικών ασφάλειας εσωτερικά αλλά και προς άλλες εξωτερικές περιοχές ασφάλειας.
Όλη η κυκλοφορία NDS/IP από τις οντότητες δικτύων της περιοχής ασφάλειας καθοδηγείται μέσω SEG σε άλλη περιοχή ασφάλειας χρησιμοποιώντας την προστασία ασφάλειας hop-by-hop στον τελικό προορισμό.

2.3.1 Διεπαφές NDS

Οι διεπαφές μεταξύ των περιοχών ασφάλειας απεικονίζονται ως Za ενώ οι διεπαφές μέσα στην περιοχή ασφάλειας αντιπροσωπεύονται ως Zb όπως φαίνεται στην Εικόνα 5. Η διεπαφή Za καλύπτει όλη την κυκλοφορία NDS/IP μεταξύ των περιοχών ασφάλειας. Για την διεπαφή Za, η επικύρωση και η προστασία ακεραιότητας δεδομένων απαιτούνται, ενώ η κρυπτογράφηση δεδομένων συνιστάται. Αυτά τα τρία χαρακτηριστικά γνωρίσματα ασφάλειας εφαρμόζονται με την χρήστη του πρωτοκόλλου ESP (Encapsulated Security Payload). Τα SEGs χρησιμοποιούνε το πρωτόκολλο IKE (Internet Key Exchange) για να διαπραγματευτούν, να δημιουργήσουν και να διατηρήσουν τούνελ ασφαλείας ESP για την αποστολή της κυκλοφορίας NDS/IP μεταξύ των περιοχών ασφάλειας. Η πολιτική ασφάλειας στην διεπαφή Za εξαρτάται από τη συμφωνία roaming. Για την διεπαφή Zb, η επικύρωση και η προστασία ακεραιότητας δεδομένων απαιτούνται και εφαρμόζονται με τη χρήση του πρωτόκολλου ESP. Η κρυπτογράφηση των δεδομένων είναι προαιρετική και εξαρτάται από την απόφαση του χειριστή των περιοχών ασφάλειας.



Εικόνα 5. **Αρχιτεκτονική ασφαλείας μεταξύ των περιοχών**

2.3.2 Πύλες ασφαλείας (SEG)

Οι πύλες ασφάλειας είναι οντότητες δικτύων στα σύνορα των περιοχών ασφάλειας IP που παρέχουν ασφάλεια σε πρωτόκολλα που βασίζονται στο IP. Όλα τα δεδομένα NDS/IP περνούν μέσω SEG πριν εισέλθουν ή αποχωρήσουν από την περιοχή ασφάλειας. Μια περιοχή ασφάλειας μπορεί να έχει περισσότερα από ένα SEG ανάλογα με τους προορισμούς, για την αποφυγή ενός μοναδικού σημείου αποτυχίας και για την εξισορρόπηση του φόρτου. Για την προστασία της κυκλοφορίας IMS μεταξύ των περιοχών είναι υποχρεωτικό να παρασχεθεί εμπιστευτικότητα, ακεραιότητα δεδομένων και η πιστοποίηση στο NDS/IP.

Οι πύλες ασφάλειας επιβάλλουν τις πολιτικές ασφάλειας μεταξύ των δικτύων. Η ασφάλεια μπορεί να συμπεριλάβει πολιτικές φιλτραρίσματος καθώς επίσης και λειτουργίες firewall. Τα SEGs είναι αρμόδια για τις ευαίσθητες διαδικασίες ασφάλειας και πρέπει να προστατεύονται. Ένα SEG θα παράσχει τουλάχιστον ένα IPSec τούνελ σε ένα άλλο ομότιμο SEG. Κάθε SEG είναι αρμόδιο για την καθιέρωση και διατήρηση των συσχετίσεων ασφάλειας IPSec (SAs) με τα ομότιμα SEGs. Τα SAs καθορίζονται χρησιμοποιώντας το πρωτόκολλο IKE. Κάθε SEG διατηρεί δύο SAs ανά σύνδεση: ένα για την εισερχόμενη κυκλοφορία και το άλλο για την εξερχόμενη κυκλοφορία. Επιπλέον, διατηρεί ένα μοναδικό ISAKMP SA (Internet Security Association and Key Management Protocol, ISAKMP) για τη διαχείριση κλειδιών. Το SEG διατηρεί μια βάση δεδομένων συσχετίσεων ασφάλειας και μια βάση δεδομένων πολιτικών ασφάλειας, για κάθε διεπαφή.

Οι λειτουργικότητες των βάσεων αυτών είναι οι εξής:

- Βάση δεδομένων πολιτικών ασφάλειας (Security Policy Database, SPD). Περιέχει τις πολιτικές σύμφωνα με τις οποίες ταξινομείται όλη η εισερχόμενη και εξερχόμενη κυκλοφορία από τις πύλες ασφάλειας. Γενικά, τα πακέτα επιλέγονται βάσει των επικεφαλίδων του επιπέδου μεταφοράς (transport layer) που συγκρίνονται με τις καταχωρήσεις στη βάση δεδομένων (SPD).

- Βάση δεδομένων συσχετίσεων ασφάλειας (Security Associations Database, SAD). Περιέχει όλα τα ενεργά SAs και σχετικές παραμέτρους. Ένα σύνολο επιλογέων (selectors) χρησιμοποιείται από την SPD για να αντιστοιχήσει την κυκλοφορία σε ένα συγκεκριμένο SA. Αυτή η σχέση αντιπροσωπεύεται από ένα σύνολο πληροφοριών μεταξύ των SEGs. Οι πληροφορίες αυτές πρέπει να συμφωνηθούν σχετικά και να διαμοιραστούν μεταξύ όλων των SEGs. Κατά την πρόσβαση των ιδιοτήτων των SA, τα

SEGs χρησιμοποιούν έναν δείκτη/προσδιοριστικό που αναφέρεται ως δείκτης παραμέτρου ασφάλειας (Security Parameter Index, SPI).

2.4 Χαρακτηριστικά ασφάλειας στις περιοχές χρήστη και εφαρμογής

2.4.1 Ασφάλεια περιοχής χρήστη

Η ασφάλεια περιοχής χρήστη εξασφαλίζει ασφαλή πρόσβαση στο MS. Βασίζεται σε μια φυσική συσκευή αποκαλούμενη κάρτα ολοκληρωμένων κυκλωμάτων UMTS, η οποία μπορεί να εισαχθεί και να αφαιρεθεί εύκολα από τον τερματικό εξοπλισμό, η οποία περιέχει εφαρμογές ασφάλειας όπως είναι το USIM. Το USIM αντιπροσωπεύει και προσδιορίζει έναν χρήστη και την σχέση του με ένα HE. Είναι αρμόδιο για την εκτέλεση της επικύρωσης συνδρομητών και δικτύων, καθώς επίσης και για τη συμφωνία κλειδιών, κατά την πρόσβαση υπηρεσιών 3G. Μπορεί επίσης να περιέχει ένα αντίγραφο του προφίλ χρήστη.

Η πρόσβαση USIM είναι περιορισμένη σε έναν εξουσιοδοτημένο χρήστη, ή σε διαφορετικούς εξουσιοδοτημένους χρήστες. Για αυτό ο χρήστης και το USIM πρέπει να μοιραστούν ένα μυστικό δεδομένο (π.χ. το PIN). Ο χρήστης αποκτά πρόσβαση στο USIM μόνο εάν γνωρίζει το μυστικό αυτό. 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.

2.4.2 Ασφάλεια περιοχής εφαρμογής

Η ασφάλεια περιοχής εφαρμογών ασχολείται με την ασφαλή ανταλλαγή μηνυμάτων μεταξύ του MS και του SN ή του SP, βάσει του επίπεδου ασφάλειας που επιλέγεται από το χειριστή του δικτύου ή τον παροχέα της εφαρμογής. Μια απομακρυσμένη εφαρμογή θα πρέπει να πιστοποιήσει έναν χρήστη πριν θα του επιτραπεί να αξιοποιήσει τις υπηρεσίες της εφαρμογής. Οι μηχανισμοί ασφάλειας σε επίπεδο εφαρμογής είναι απαραίτητοι διότι η λειτουργικότητα των χαμηλότερων στρωμάτων δεν μπορεί να εγγυηθεί την end-to-end παροχή

ασφάλειας. Έλλειψη end-to-end ασφάλειας θα μπορούσε να προβλεφθεί όταν, για παράδειγμα, το απομακρυσμένο μέρος είναι προσβάσιμο μέσω του Διαδικτύου.

Το USIM Application Toolkit παρέχει τη δυνατότητα για τρίτους φορείς ή παρόχους υπηρεσιών να δημιουργήσουν εφαρμογές που είναι μόνιμες στην USIM. Για να διασφαλιστούν οι ασφαλείς συναλλαγές μεταξύ του MS και του SN ή του SP, μια σειρά από βασικούς μηχανισμούς ασφάλειας, όπως η πιστοποίηση οντότητας, αυθεντικότητα μηνύματος, ανίχνευση επανάληψης (replay), διαβεβαίωση εμπιστευτικότητας, και απόδειξη παραλαβής, έχουν προσδιοριστεί και ενσωματώνονται στο USIM Application Toolkit.

Το Πρωτόκολλο Ασύρματων Εφαρμογών (Wireless Application Protocol, WAP) είναι μια σουίτα προτύπων για την παράδοση και την παρουσίαση των υπηρεσιών του Διαδικτύου σε ασύρματα τερματικά, λαμβάνοντας υπόψη το περιορισμένο εύρος ζώνης των δικτύων κινητής τηλεφωνίας, καθώς και τις περιορισμένες δυνατότητες επεξεργασίας των κινητών συσκευών. Για την σύνδεση του ασύρματου δικτύου στο Internet, μια πύλη WAP είναι απαραίτητη για να μεταφράσει τα πρωτόκολλα που χρησιμοποιούνται στο WAP σε πρωτόκολλα που χρησιμοποιούνται στο Internet. Η αρχιτεκτονική WAP έχει τυποποιηθεί σε δύο κυκλοφορίες (εκδόσεις 1.2.1 και 2.0). Για να εξασφαλιστεί η μετάδοση δεδομένων στην αρχιτεκτονική WAP (έκδοση 1.2.1), το ασύρματο πρωτόκολλο ασφάλειας στρώματος μεταφορών (Wireless Transport Layer Security, WTLS), που είναι βασισμένο στο πρωτόκολλο TLS, υιοθετείται. Το WTLS έχει βελτιστοποιηθεί για τη χρήση μέσα από κανάλια επικοινωνίας περιορισμένου εύρους που παρέχουν επίσης υποστήριξη για datagram. Εξασφαλίζει την ακεραιότητα δεδομένων, τη μυστικότητα, την επικύρωση και προστασία από επίθεση denial-of-service. Για τις εφαρμογές Ιστού που υιοθετούν τεχνικές ασφάλειας Διαδικτύου μέσω του TLS, η πύλη WAP αυτόματα και διαφανώς διαχειρίζεται την ασύρματη ασφάλεια και μεταβιβάζει τα προστατευμένα δεδομένα μεταξύ των καναλιών ασφάλειας WTLS και TLS. Κατά συνέπεια, αυτή η αρχιτεκτονική δεν υποστηρίζει end-to-end ασφάλεια.

Το WAP 2.0 προχωρά στον επανασχεδιασμό της αρχιτεκτονικής WAP με την εισαγωγή της υπάρχουσας στοίβας πρωτοκόλλων του Διαδικτύου, συμπεριλαμβανομένου του πρωτοκόλλου ελέγχου μετάδοσης (TCP) στο περιβάλλον WAP. Η νέα αρχιτεκτονική επιτρέπει μια σειρά διαφορετικών πυλών, η οποία επιτρέπει τη μετατροπή μεταξύ των δύο πρωτοκόλλων. Μια πύλη, σε επίπεδο TCP επιτρέπει δύο εκδόσεις του TCP, μια για ενσύρματο και η άλλη για το ασύρματο δίκτυο, πάνω από την οποία ένα ασφαλές κανάλι TLS μπορεί να καθιερωθεί από την κινητή συσκευή στον διακομιστή.

2.4.3 Διαφάνεια και διαμόρφωση ασφάλειας

Αν και τα μέτρα ασφάλειας που παρέχονται από το SN πρέπει να είναι διαφανή στον τελικό χρήστη, η διαφάνεια των διαδικασιών ασφάλειας καθώς επίσης και των υποστηριζόμενων χαρακτηριστικών ασφάλειας πρέπει να είναι ορατή.
Συνεπώς πρέπει να παρέχεται:

- ένδειξη της κρυπτογράφησης στην πρόσβαση δικτύων.
- ένδειξη της κρυπτογράφησης σε όλο το δίκτυο.
- ένδειξη του επιπέδου ασφάλειας (π.χ. όταν ένας χρήστης μετακινείται από το 3G σε 2G).

Η δυνατότητα διαμόρφωσης (Configurability) επιτρέπει στον κινητό χρήστη και στο HE να διαμορφώσουν εάν μια παροχή υπηρεσιών πρέπει να εξαρτηθεί από την ενεργοποίηση ορισμένων χαρακτηριστικών ασφάλειας. Μια υπηρεσία μπορεί να χρησιμοποιηθεί μόνο όταν είναι όλα τα σχετικά χαρακτηριστικά γνωρίσματα ασφάλειας σε λειτουργία. Τα χαρακτηριστικά γνωρίσματα που μπορούν να διαμορφωθούν είναι:

- ενεργοποίηση / απενεργοποίηση πιστοποίησης του χρήστη USIM για ορισμένες υπηρεσίες.
- Αποδοχή / απόρριψη για τις εισερχόμενες μη-κρυπτογραφημένες κλήσεις.
- αποδοχή / απόρριψη της χρήσης ορισμένων αλγορίθμων κρυπτογράφησης.

2.5 Ασφάλεια στο UMTS και Νόμιμη υποκλοπή

Σε αυτό το κεφάλαιο παρουσιάστηκαν οι απαιτούμενες μέθοδοι και ενέργειες για την αποτελεσματική αντιμετώπιση των απειλών ασφάλειας. Αναλύθηκαν οι μέθοδοι και οι τεχνικές ασφάλειας στα επιμέρους τμήματα του δικτύου που αφορούν την προστασία του καθώς και την προστασία των χρηστών.

Ένα άλλο σκέλος της ασφάλειας στο UMTS αφορά την δυνατότητα νόμιμης υποκλοπής (lawful interception, LI) από εξουσιοδοτημένες αρχές. Η νόμιμη υποκλοκή διαδραματίζει κρίσιμο ρόλο στη βοήθεια των αρχών επιβολής του νόμου για να καταπολεμηθεί η εγκληματική

δραστηριότητα. Η νόμιμη υποκλοκή στα δημόσια συστήματα τηλεπικοινωνιών σε κάθε χώρα είναι βασισμένη στην εθνική νομοθεσία της χώρας. Συνεπώς είναι επιτακτική η ανάγκη τυποποίησης της νόμιμης υποκλοκής και ενσωμάτωσης της στα δίκτυα κινητής τηλεφωνίας. Στο επόμενο κεφάλαιο παρουσιάζονται αναλυτικά οι τροποποιήσεις στο UMTS για την υποστήριξη της νόμιμης υποκλοπής.

Αναφορές κεφαλαίου

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

[2] http://www.cs.uoi.gr/~cs040909/page6.html

[2] *An Approach to full User Data Integrity Protection in UMTS Access Networks*

Κεφάλαιο 3

3.1 Συγκεκριμένα προσδιοριστικά για το LI

Τα συγκεκριμένα προσδιοριστικά (identifiers) είναι απαραίτητα για να προσδιορίσουν μοναδικά έναν στόχο για υποκλοπή (interception) και για να συσχετίσουν τα δεδομένα, το οποία μεταβιβάζονται διαμέσου διαφορετικών διεπαφών μεταβίβασης (Handover Interfaces, HI1, HI2 και HI3). Τα προσδιοριστικά, που ισχύουν για όλες τις τεχνολογίες επικοινωνιών, ορίζονται στις παρακάτω ενότητες.

3.1.1 Προσδιοριστικό νόμιμης υποκλοπής (LIID)

Για κάθε ταυτότητα-στόχο που σχετίζεται με ένα μέτρο υποκλοπής (interception measure), ο εξουσιοδοτημένος χειριστής (NO/AN/SP) θα ορίσει ένα ειδικό **προσδιοριστικό νόμιμης υποκλοπής** (Lawful Interception Identifier, LIID), το οποίο έχει συμφωνηθεί μεταξύ του LEA και του χειριστή (NO/AN/SP). Χρησιμοποιείται μέσα στις παραμέτρους όλων των διεπαφών HI. Η χρησιμοποίηση ενός έμμεσου προσδιορισμού, που δείχνει μια ταυτότητα στόχων το καθιστά ευκολότερο να κρατήσει τη γνώση για έναν συγκεκριμένο στόχο παρεμπόδισης που περιορίζεται μέσα στους εξουσιοδοτημένους χειριστές (NO/AN/SP) και τους διαχειριζόμενους πράκτορες στο LEA.

Το LIID είναι ένα συστατικό της διαδικασίας παράδοσης CC (Content of Communication) και των εγγραφών IRI. Θα χρησιμοποιηθεί όταν ανταλλάσσονται δεδομένα στις διεπαφές παράδοσης HI2 και HI3 για λόγους ταυτοποίησης και συσχετισμού.

Η μορφή LIID θα αποτελείται από αλφαριθμητικούς χαρακτήρες. Παραδείγματος χάριν, μεταξύ άλλων πληροφοριών, θα περιέχει και έναν νόμιμο αριθμό αναφοράς εξουσιοδότησης και την ημερομηνία που εκδόθηκε η νόμιμη εξουσιοδότηση.

Ο εξουσιοδοτημένος χειριστής (NO/AN/SP) θα εισαγάγει, για κάθε ταυτότητα-στόχο του υποκειμένου υποκλοπής, ένα μοναδικό LIID. Εάν περισσότερα από ένα LEA υποκλέπτουν την ίδια ταυτότητα-στόχο, θα υπάρξουν μοναδικά LIIDs, που θα σχετίζονται με κάθε LEA.

3.1.2 Προσδιοριστικό επικοινωνίας (CID)

Για κάθε δραστηριότητα σχετική με μια ταυτότητα-στόχο, παράγεται ένα CID από το σχετικό τμήμα του δικτύου. Το CID αποτελείται από τα ακόλουθα δύο προσδιοριστικά:

- ID δίκτυου (Network ID, NID)
- αριθμός ταυτότητας επικοινωνίας (Communication Identity Number, CIN) - προαιρετικό.

Για όλες τις μη σχετικές εγγραφές CC όπως SMS, SCI κ.λ.π δεν θα μπορούσε να γίνει κανένας συσχετισμός με ένα CC.

Το CID διακρίνει μεταξύ των διαφορετικών δραστηριοτήτων της ταυτότητας-στόχου. Χρησιμοποιείται επίσης για το συσχετισμό μεταξύ των εγγραφών IRI και των συνδέσεων CC, καθώς επίσης και στα HI2 και HI3.

3.1.2.1 Προσδιοριστικό δικτύου (NID)

Το **προσδιοριστικό δικτύου** είναι μια υποχρεωτική παράμετρος και πρέπει να είναι διεθνώς μοναδικό. Αποτελείται από ένα ή και τα δύο από τα ακόλουθα δύο προσδιοριστικά.

- Προσδιοριστικό χειριστή (υποχρεωτικό): Μοναδικός προσδιορισμός του χειριστή δικτύων, του παρόχου δικτύου πρόσβασης ή του παρόχου υπηρεσιών.
- προσδιοριστικό στοιχείων δικτύου (Network element identifier, NEID) (προαιρετικό): Ο σκοπός του προσδιοριστικού στοιχείων δικτύου είναι να προσδιοριστεί μοναδικά το σχετικό

στοιχείο δικτύου που διενεργεί τις λειτουργίες LI, όπως η ενεργοποίηση LI, η αποστολή της εγγραφής IRI, κ.λπ.

Ένα προσδιοριστικό στοιχείων δικτύου μπορεί να είναι:

- ένας διεθνής αριθμός E.164 κόμβων
- μια διεύθυνση X.25
- μια διεύθυνση IP.

3.1.2.2 Αριθμός ταυτότητας επικοινωνίας (Communication Identity Number, CIN)

Αυτή η παράμετρος είναι υποχρεωτική για το IRI σε περίπτωση γεγονότων αναφοράς (reporting events) για επικοινωνίες βασισμένες σε σύνδεση (π.χ. circuit switched).

Ο αριθμός ταυτότητας επικοινωνίας είναι ένα προσωρινό προσδιοριστικό μιας επικοινωνίας που έχει υποκλαπεί και είναι σχετική με μια συγκεκριμένη ταυτότητα-στόχο.

3.1.3 Προσδιοριστικό συνδέσεων CC (CC link identifier, CCLID)

Αυτό το προσδιοριστικό χρησιμοποιείται μόνο στις διεπαφές HI2 και HI3 σε περίπτωση επαναχρησιμοποίησης των συνδέσεων CC. Για κάθε σύνδεση CC, που πραγματοποιείται από τη συνάρτηση μεσολάβησης (mediation function) προς το LEMF, ένα προσδιοριστικό συνδέσεων CC (CCLID) διαβιβάζεται στις εγγραφές της HI2 και στο μήνυμα εγκατάστασης του HI3, επιπρόσθετα με τα CIN και NID. Για το σωστό συσχετισμό των πολυμερών κλήσεων, αυτός ο αριθμός ταυτότητας προσδιορίζει στις εγγραφές IRI κάθε κλήσης, ποια σύνδεση CC χρησιμοποιείται για τη μετάδοση του CC.

Το CCLID μπορεί να χρησιμοποιήσει την ίδια μορφή με το CIN και σε αυτήν την περίπτωση δεν χρειάζεται να διαβιβαστεί ρητά κατά τη διάρκεια της εγκατάστασης των συνδέσεων CC, ως τμήμα του HI3. Το CIN μπορεί επίσης έμμεσα να αντιπροσωπεύσει το CCLID.

3.1.4 Ο συσχετισμός των CC και IRI

Για να διαβεβαιωθεί ο συσχετισμός μεταξύ του ανεξάρτητα μεταβιβασθέντος περιεχομένου της επικοινωνίας (Content of Communication, CC) και των πληροφοριών IRI (Intercept Related Information) μιας κλήσης, χρησιμοποιούνται οι ακόλουθες παράμετροι:

- Το προσδιοριστικό νόμιμης υποκλοπής (LIID)
- Το προσδιοριστικό επικοινωνίας (CID)
- Το προσδιοριστικό συνδέσεων CC (CCLID),

Αυτές οι παράμετροι μεταφέρονται από το MF στο LEMF στα HI2 και HI3.

Για κάθε κλήση ή άλλη δραστηριότητα σχετικά με μια ταυτότητα-στόχο, παράγεται ένα CID από το σχετικό στοιχείο του δικτύου. Το CID αποτελείται από τα ακόλουθα δύο προσδιοριστικά:

- Προσδιοριστικό δικτύου (NID)
- Αριθμός ταυτότητας επικοινωνίας (CIN).

Στο σύστημα UMTS χρησιμοποιείται η ταυτότητα κόμβου υποκλοπής για το NID.

Ο αριθμός συσχετισμού χρησιμοποιείται για το CIN. Για το προσδιοριστικό επικοινωνίας (CID) στο σύστημα UMTS χρησιμοποιείται ο συνδυασμός της ταυτότητας του κόμβου υποκλοπής και του αριθμού συσχέτισης.

3.1.5 Η χρήση των προσδιοριστικών

Τα προσδιοριστικά ανταλλάσσονται μεταξύ της συνάρτησης μεσολάβησης και του LEMF μέσω των διεπαφών HI1, HI2 και HI3. Υπάρχουν διάφορες επιλογές διεπαφών για την ανταλλαγή των πληροφοριών. Οι πίνακες 1 και 2 καθορίζουν τη χρήση των αριθμών και των προσδιοριστικών ανάλογα με αυτές τις επιλογές.

ΣΗΜΕΙΩΣΗ: Το X στους πίνακες 1 και 2 καθορίζει το προσδιοριστικό που χρησιμοποιείται μέσα στις παραμέτρους της διεπαφής.

Προσ-διοριστικό	**IRI και CC που μεταβιβάζονται (επιλογή A)**			**IRI και CC που μεταβιβάζονται (επιλογή B)**		
	HI1	**HI2**	**HI3**	**HI1**	**HI2**	**HI3**
LIID	X	X	X	X	X	X
NID		X	X		X	X
CIN		X	X		X	X (σημ. 1)
CCLID					X	X (σημ. 2)
Σημ. 1: Το CIN της πρώτης κλήσης για την οποία η σύνδεση CC έχει εγκατασταθεί. Σημ. 2: Το CCLID μπορεί να παραληφθεί.						

Πίνακας 1: Χρήση των προσδιοριστικών και των IRI και CC που μεταβιβάζονται.

Προσδιοριστικό	Μεταβιβάζεται μόνο το IRI	
	HI1	HI2
LIID	X	X
NID		X
CIN		X
CCLID		

Πίνακας 2: Χρήση προσδιοριστικών

3.2 Διεπαφή HI2 για IRI

3.2.1 Ο ορισμός του IRI

Οι σχετικές πληροφορίες με την υποκλοπή (IRI) θα είναι σε γενικές γραμμές διαθέσιμες στις ακόλουθες φάσεις μιας κλήσης (επιτυχούς ή όχι):

1) Στην έναρξη της κλήσης όταν η ταυτότητα-στόχος γίνεται ενεργή, οι πληροφορίες προορισμού κλήσης μπορεί να είναι ή όχι διαθέσιμες.

2) Στο τέλος μιας κλήσης, όταν η ταυτότητα-στόχος γίνεται ανενεργή (φάση απελευθέρωσης της κλήσης).

3) Σε συγκεκριμένες στιγμές μεταξύ των ανωτέρω φάσεων, όταν οι σχετικές πληροφορίες γίνονται διαθέσιμες (ενεργός φάση κλήσης).

Επιπλέον, οι πληροφορίες για τις ενέργειες ενός στόχου, που δεν σχετίζονται με την κλήση, αποτελούν το IRI και στέλνονται μέσω HI2.

Το IRI μπορεί να υποδιαιρεθεί στις ακόλουθες κατηγορίες:

1) Πληροφορίες ελέγχου για το HI2 (π.χ. πληροφορίες συσχετισμού).

2) Βασικές πληροφορίες κλήσης, για τις κλήσεις μεταξύ δύο συμβαλλόμενων μερών.

3) Πληροφορίες που αφορούν τις συμπληρωματικές υπηρεσίες, οι οποίες έχουν χρησιμοποιηθεί κατά τη διάρκεια μιας κλήσης.

4) Πληροφορίες για τις ενέργειες στόχου που δεν σχετίζονται με την κλήση.

3.2.2 Η δομή των εγγραφών IRI

Κάθε εγγραφή IRI περιέχει διάφορες παραμέτρους. Οι υποχρεωτικές παράμετροι καθορίζονται ως πληροφορίες ελέγχου του HI2. Οι προαιρετικές παράμετροι παρέχονται ανάλογα με τη διαθεσιμότητα στο MF. Για την εσωτερική δομή των εγγραφών IRI, χρησιμοποιείται η περιγραφή ASN.1 με την εφαρμογή των βασικών κανόνων κωδικοποίησης (basic encoding rules , BER).

3.2.2.1 Πληροφορίες ελέγχου για το HI2

Ο κύριος σκοπός αυτών των πληροφοριών είναι ο μοναδικός προσδιορισμός των εγγραφών που σχετίζονται με μια ταυτότητα-στόχο, συμπεριλαμβανομένης της χαρτογράφησης στις συνδέσεις CC. Γενικά, οι παράμετροι αυτής της κατηγορίας είναι υποχρεωτικές, δηλ. πρέπει να παρασχεθούν με οποιαδήποτε εγγραφή.

Ορίζονται τα ακόλουθα στοιχεία:

1) Ο τύπος εγγραφής (IRIContent). Τύποι εγγραφών: IRI-BEGIN, IRI-CONTINUE, IRI-END, IRI-REPORT

2) Ένδειξη έκδοσης (IRIversion). Προσδιορισμός της έκδοσης της προδιαγραφής διεπαφών HI2

3) Προσδιοριστικό επικοινωνίας (CID).

4) Προσδιοριστικό νόμιμης υποκλοπής (LIID).

5) Ημερομηνία και χρόνος (TimeStamp)

Η ημερομηνία και ο χρόνος της συνθήκης ενεργοποίησης εγγραφής (record trigger condition). Η παράμετρος θα έχει την ικανότητα να υποδείξει εάν οι χρονικές πληροφορίες δίνονται ως Τοπική ώρα χωρίς χρονική ζώνη ή ως UTC. Κανονικά ο χειριστής (NO/AN/SP) θα καθορίσει αυτές τις επιλογές.

6) Προσδιοριστικό συνδέσεων CC (*CC-Link-Identifier*).

Ο πίνακας 3 συνοψίζει τα στοιχεία των πληροφοριών ελέγχου του HI2. Όλες αυτές οι πληροφορίες είναι υποχρεωτικές, εκτός από το CID, που μπορεί να παραλειφθεί για τις non-call

εγγραφές IRI, και το CCLID. Ο καθορισμός της μορφής και της κωδικοποίησης τους σχετίζεται με το LI.

Παράμετροι IRI: Πληροφορίες ελέγχου LI	
Όνομα παραμέτρου IRI	**Όνομα ASN.1**
Type of record	IRIContent
Version indication	iRIversion
Lawful Interception IDentifier (LIID)	LawfulInterceptionIdentifier
Communication IDentifier (CID) - Communication Identity Number (CIN) - Network IDentifier (NID)	CommunicationIdentifier
Date & time	TimeStamp
CC Link IDentifier (CCLID) (only used in case of option B)	CC-Link-Identifier

Πίνακας 3: Παράμετροι για τις πληροφορίες ελέγχου LI στις εγγραφές IRI (διεπαφή HI2)

3.2.2.2 Πληροφορίες βασικής κλήσης

Ορίζουν τις παραμέτρους μέσα στις εγγραφές IRI για τις βασικές κλήσεις, δηλ. κλήσεις, για τις οποίες κατά τη διάρκεια τους δεν έχει χρησιμοποιηθεί καμία συμπληρωματική υπηρεσία. Γενικά, οι παράμετροι συσχετίζονται με τα συμβαλλόμενα μέρη μιας κλήσης, συνεπώς τα ASN.1 containers καθορίζονται για τους τύπους των συμβαλλόμενων μερών, οι οποίοι επιτρέπουν να συμπεριληφθούν οι σχετικές τους πληροφορίες.

Τα παρακάτω στοιχεία πρόκειται να συμπεριληφθούν όταν διατίθενται για πρώτη φορά κατά τη διάρκεια μιας κλήσης υπό εξέλιξη. Εάν το ίδιο στοιχείο εμφανίζεται όμοιο αρκετές φορές κατά τη διάρκεια μιας κλήσης, πρέπει να διαβιβαστεί μόνο μία φορά, π.χ σε μια εγγραφή IRI-BEGIN:

1) Κατεύθυνση της κλήσης (*intercepted-Call-Direct*). Προσδιορίζει εάν η ταυτότητα-στόχος αποτελεί το συμβαλλόμενο μέρος της προέλευσης (originating party) ή του τερματισμού (terminating party) .

2) Διεύθυνση του μέρους προέλευσης και τερματισμού (CallingPartyNumber ή CalledPartyNumber).

3) Βασική υπηρεσία, LLC (*Services-Information*). Οι παράμετροι όπως παραλαμβάνονται από το πρωτόκολλο σηματοδότησης (π.χ. BC., HLC, TMR, LLC).

4) Αιτία (*ISUP-parameters* ή *DSS1-parameters-codeset-0*). Ο λόγος για την απελευθέρωση της κλήσης που υποκλέπτεται. Η τιμή αυτή παραλαμβάνεται από το πρωτόκολλο σηματοδότησης και διαβιβάζεται με το ASN.1 container του συμβαλλόμενου μέρους, το οποίο άρχισε την απελευθέρωση.

5) Πρόσθετες παράμετροι δικτύων. Για παράδειγμα, πληροφορίες θέσης (*Location*).

Οι παράμετροι που καθορίζονται στον πίνακα 4.5 θα χρησιμοποιηθούν για τις υπάρχουσες υπηρεσίες, με το δεδομένη μορφή 3GPP. Μπορούν να εφαρμοστούν εθνικές επεκτάσεις (national extensions) χρησιμοποιώντας την παράμετρο ASN.1 *National-Parameters*.

3.2.2.3 Πληροφορίες για τις συμπληρωματικές υπηρεσίες, σχετικές με μια κλήση υπό εξέλιξη

Η γενική αρχή είναι να γίνεται η μεταβίβαση των πληροφοριών σχετικών με μια υπηρεσία μέσα στις εγγραφές IRI όταν παραλαμβάνονται οι αντίστοιχες πληροφορίες, που πρέπει να μεταβιβαστούν στο LEMF, από το πρωτόκολλο σηματοδότησης. Όπου είναι δυνατόν, η κωδικοποίηση των σχετικών πληροφοριών θα χρησιμοποιήσει την ίδια μορφή όπως καθορίζεται από τα τυποποιημένα πρωτόκολλα σηματοδότησης.

Η επιλογή των τύπων των γεγονότων ή των πληροφοριών που είναι σχετικές για τη μετάδοση στα LEAs, συμβαδίζει με τις απαιτήσεις που καθορίζονται στα [1] και [2].

Μια παράμετρος ASN.1 καθορίζεται για τις συμπληρωματικές υπηρεσίες που είναι σχετικές με τις κλήσεις προώθησης ή επαναδρομολόγησης (πληροφορίες *forwarded-to-Party*), λόγω της σχέσης αυτού του είδους υπηρεσιών όσον αφορά το LI. Για τις διάφορες περιπτώσεις των προωθημένων κλήσεων, οι σχετικές πληροφορίες συμπεριλαμβάνονται στις πληροφορίες *originatingParty*/*terminatingParty*/*forwarded-to-Party*:

1) Εάν μια κλήση στο στόχο έχει προηγουμένως προωθηθεί, οι διαθέσιμες παράμετροι σχετικά με το συμβαλλόμενο μέρος επαναπροώθησης ενθυλακώνονται μέσα στην παράμετρο *originatingPartyInformation*.

2) Εάν η κλήση διαβιβάζεται στην πρόσβαση του στόχου, οι παράμετροι που συσχετίζονται με το συμβαλλόμενο μέρος επαναπροώθησης (στόχος) είναι ενθυλακωμένες μέσα στην παράμετρο *terminatingPartyInformation*.

3) Όλες οι παράμετροι που είναι σχετικές με συμβαλλόμενο μέρος στο οποίο γίνεται η προώθηση είναι ενσωματωμένες μέσα στην παράμετρο ASN1 *forwarded-to-Party*. Επιπλέον, αυτή η παράμετρος περιλαμβάνει το *supplementary-Services-Information* που περιέχει την διεύθυνση *forwarded-to* και την παράμετρο πληροφοριών προώθησης, με το λόγο της προώθησης της κλήσης, κ.λπ.

3.2.2.4 πληροφορίες για τις non-call συμπληρωματικές υπηρεσίες

Η γενική αρχή είναι να διαβιβαστούν οι non-call πληροφορίες των υπηρεσιών όπως παραλαμβάνονται από το πρωτόκολλο σηματοδότησης. Μια χαρακτηριστική ενέργεια χρηστών που αναφέρεται είναι η ελεγχόμενη εισαγωγή συνδρομητή (Subscriber Controlled Input, SCI).

3.2.3 Παράδοση του IRI

Τα γεγονότα που καθορίζονται στο [19] χρησιμοποιούνται για να παραγάγουν τις εγγραφής για την παράδοση μέσω HI2. Υπάρχουν οκτώ διαφορετικοί τύποι γεγονότων που παραλαμβάνονται σε επίπεδο DF2. Σύμφωνα με το κάθε γεγονός, μια εγγραφή στέλνεται στο LEMF εάν αυτή απαιτείται. Ο ακόλουθος πίνακας δίνει τη χαρτογράφηση μεταξύ του τύπου γεγονότος που παραλαμβάνονται σε επίπεδο DF2 και του τύπου εγγραφής που στέλνεται στο LEMF. Αποτελεί επιλογή της υλοποίησης το εάν οι πλεονάζουσες πληροφορίες θα σταλούν για κάθε περαιτέρω γεγονός.

Γεγονός	**Τύπος εγγραφής IRI**
Call establishment	BEGIN
Answer	CONTINUE
Supplementary service	CONTINUE
Handover	CONTINUE
Release	END
Location update	REPORT
Subscriber controlled input	REPORT
SMS	REPORT

Πίνακας 4: Δομή των εγγραφών για το UMTS (CS)

Ένα σύνολο πληροφοριών χρησιμοποιείται για να παραγάγει τις εγγραφές. Αυτές οι εγγραφές χρησιμοποιούνται για να διαβιβάζουν τις πληροφορίες από τη συνάρτηση μεσολάβησης στο LEMF. Αυτό το σύνολο πληροφοριών μπορεί να επεκταθεί στον διακομιστή 3G MSC ή στον 3G GMSC ή στο DF2/MF, εάν αυτό είναι απαραίτητο σε μια συγκεκριμένη χώρα. Ο ακόλουθος πίνακας δίνει τη χαρτογράφηση μεταξύ των πληροφοριών που παραλαμβάνονται ανά γεγονός και των πληροφοριών που στέλνονται στις εγγραφές

Παράμετρος	Ορισμός	Παράμετρος ASN.1
observed MSISDN	Target Identifier with the MSISDN of the target subscriber (monitored subscriber)	PartyInformation/msISDN
observed IMSI	Target Identifier with the IMSI of the target subscriber (monitored subscriber)	PartyInformation/imsi
observed IMEI	Target Identifier with the IMEI of the target subscriber (monitored subscriber), it must be checked for each call over the radio interface	PartyInformation/imei
event type	Description which type of event is delivered: Establishment, Answer, Supplementary service, Handover, Release, SMS, Location update, Subscriber controlled input	There is no one-to-one mapping for this information. Parameters presence on HI2 indicates the event type (e.g. SMS or sciData parameter presence)
event date	Date of the event generation in the 3G MSC server or 3G GMSC server	Timestamp
event time	Time of the event generation in the 3G MSC server or 3G GMSC server	
dialled number	Dialled number before digit modification, IN-modification, etc.	PartyInformation (= originating)/DSS1-parameters/calledpartynumber
connected number	Number of the answering party	PartyInformation/supplementary-Services-Info
other party address	Directory number of the other party for originating calls Calling party for terminating calls	PartyInformation (= terminating)/calledpartynumber PartyInformation/callingpartynumber
call direction	Information if the monitored subscriber is calling or called e.g. MOC/MTC or originating/terminating in or/out	intercepted-Call-Direct
CID	Unique number for each call sent to the DF, to help the LEA, to have a correlation between each call and the IRI (combination of Interception Node ID and the correlation number)	communicationIdentifier
lawful interception identifier	Unique number for each surveillance lawful authorization	LawfulInterceptionIdentifier
SAI	SAI of the target; for the location information	locationOfTheTarget
location area code	Location-area-code of the target defines the Location Area in a PLMN	
basic service	Information about Tele service or bearer service	PartyInformation/DSS1-parameters-codeset-0
supplementary service	Supplementary services used by the target e.g. CF, CW, ECT	PartyInformation/Supplementary-Services
forwarded to number	Forwarded to number at CF	PartyInformation/calledPartyNumber (party-Qualifier indicating forwarded-to-party)
call release reason	Call release reason of the target call	Release-Reason-Of-intercepted-Call
SMS	The SMS content with header which is sent with the SMS-service	SMS
SCI	Non-call related Subscriber Controlled Input (SCI) which the 3G MSC server receives	PartyInformation/sciData

	from the ME	

Πίνακας 5: Περιγραφή των παραμέτρων

3.3 HI3: διεπαφή για το CC

Η διεπαφή HI3 θα μεταφέρει το περιεχόμενο της επικοινωνίας (CC) της τηλεπικοινωνιακής υπηρεσίας υποκλοπής στο LEMF. Το περιεχόμενο της επικοινωνίας θα παρουσιαστεί ως ένα διαφανές αντίγραφο της ροής πληροφοριών κατά τη διάρκεια μιας καθιερωμένης, συχνά αμφίδρομης, επικοινωνίας του αντικειμένου. Μπορεί να περιέχει φωνή ή δεδομένα. Μια κλήση στόχος έχει δυο κατευθύνσεις της μετάδοσης που σχετίζονται με αυτήν. Μια προς τον στόχο και μια από το στόχο. Απαιτούνται δύο κανάλια επικοινωνίας στο LEMF για τη μετάδοση του περιεχομένου της επικοινωνίας (στερεοφωνική μετάδοση). Το δίκτυο δεν καταγράφει και δεν αποθηκεύει το περιεχόμενο της επικοινωνίας.

3.3.1 Παράδοση του περιεχομένου της επικοινωνίας.

Κατ'εξαίρεση τα SMS θα παραδίδονται μέσω HI2. Το μέσο μετάδοσης που χρησιμοποιείται για να υποστηρίξει το HI3 θα είναι τυποποιημένες κλήσεις ISDN, βασισμένες σε συνδέσεις 64 kbit/s circuit switched. Οι συνδέσεις των CC εγκαθίστανται μετά από απαίτηση στο LEMF. Το LEMF αποτελεί μια λειτουργία χρηστών ISDN DSS1. Μπορεί να συνδεθεί τοπικά με τον κόμβο-στόχο, ή μπορεί να βρεθεί κάπου στο δίκτυο-στόχο ή σε ένα άλλο δίκτυο, με ή χωρίς την μεσολάβηση ενός ενδιάμεσου δίκτυου.

Για τη σηματοδότηση δίκτυου, θα χρησιμοποιηθεί το συνηθισμένο ISDN και δεν θα απαιτηθεί καμία τροποποίηση των υπαρχόντων πρωτοκόλλων ISDN. Οποιεσδήποτε πληροφορίες που απαιτούνται για το LI, όπως ο συσχετισμός με τις εγγραφές IRI μιας κλήσης, μπορούν να εισαχθούν στα υπάρχουσα μηνύματα και παραμέτρους χωρίς την ανάγκη να επεκταθούν τα πρωτόκολλα ETSI για την εφαρμογή LI.

Για κάθε ενεργοποίηση LI, ορίζεται μια σταθερή διεύθυνση LEMF . Αυτή η διεύθυνση δεν χρησιμοποιείται για λόγους προσδιορισμού. Ο προσδιορισμός και ο συσχετισμός των

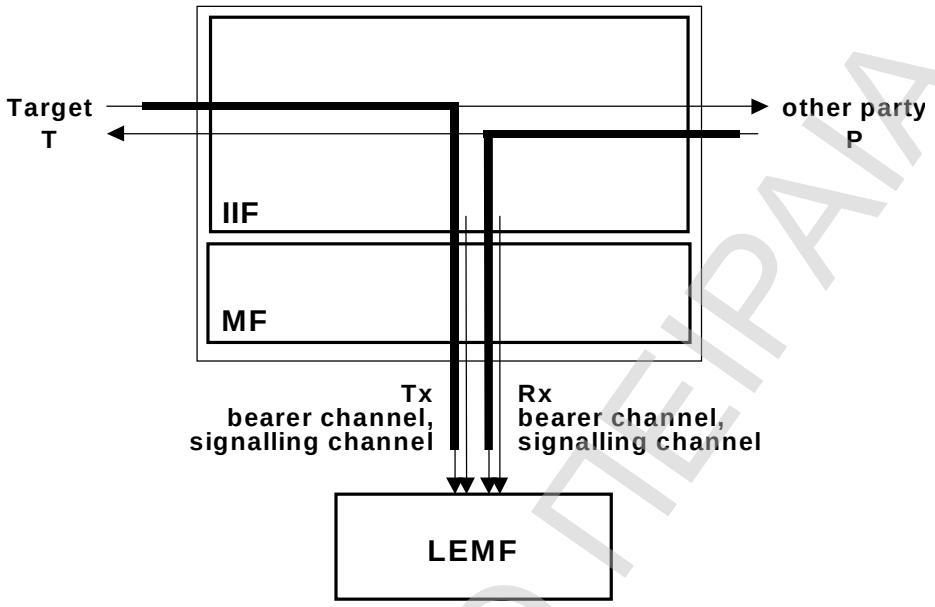
συνδέσεων CC εκτελούνται ξεχωριστά. Οι λειτουργίες που καθορίζονται στο πρότυπο ISDN χρηστών, έκδοση 1 (ETSI ISUP V1) απαιτούνται ως ελάχιστο μέσα στο δίκτυο-στόχο για την υποστήριξη:

- Του συσχετισμού των πληροφοριών HI3 στις πληροφορίες του άλλου HI, που χρησιμοποιεί τη συμπληρωματική υπηρεσία UUS1 (user-to-user signalling 1 implicit, UUS1).

- Επαλήθευση πρόσβασης της κλήσης παράδοσης.
- Η ικανότητα των φορέων που χρησιμοποιείται για τις συνδέσεις CC είναι 64 KBIT/s ψηφιακών πληροφοριών. Αυτός ο τύπος εγγυάται ότι τις πληροφορίες περνούν διαφανώς στο LEMF. Δεν απαιτείται καμία συγκεκριμένη παράμετρος HLC.
- Το κανάλι επικοινωνίας CC είναι μια μονόδρομη σύνδεση, από το IIF του χειριστή (NO/AN/SP) στο LEMF.

Το σενάριο για την παράδοση του περιεχομένου της επικοινωνίας (CC) είναι το ακόλουθο:

Στην έναρξη προσπάθειας κλήσης, για μια 64 kbit/s αμφίδρομη κλήση στόχου, δύο κλήσεις παράδοσης ISDN πραγματοποιούνται από το MF στο LEMF. Μια κλήση προσφέρει το CC προς την ταυτότητα-στόχο (κλήση/κανάλι CC Rx), η άλλη κλήση προσφέρει το CC από την ταυτότητα-στόχο (κλήση/κανάλι CC Tx). Κατά τη διάρκεια της καθιέρωσης κάθε μιας από αυτές τις κλήσεις, γίνονται οι απαραίτητοι έλεγχοι. Το MF μεταβιβάζει το LIID και το CID στο LEMF, κατά τη διάρκεια της καθιέρωσης της κλήσης, μέσα στα στοιχεία του πρωτοκόλλου σηματοδότησης της σύνδεσης CC. Το LEMF χρησιμοποιεί αυτές τις πληροφορίες για να προσδιορίσει την ταυτότητα-στόχο και για να συσχετίσει το IRI με το CC.
Στο τέλος μιας προσπάθειας κλήσης, κάθε κλήση παράδοσης που συνδέεται με αυτήν την προσπάθεια κλήσης θα απελευθερωθεί από το MF.



Εικόνα 1: Μεταβίβαση του CC από το MF στο LEMF

3.3.2 Πληροφορίες ελέγχου για το περιεχόμενο της επικοινωνίας.

Οι κλήσεις παράδοσης θα χρησιμοποιήσουν τα πρωτόκολλα ISDN χωρίς τροποποιήσεις (DSS1, ISDN user part). Ο πίνακας 6 συνοψίζει τις συγκεκριμένες ρυθμίσεις των παραμέτρων για τις συνδέσεις CC. Η παράμετρος UUS1 χρησιμοποιείται κατά τη διάρκεια της κλήσης που εγκαθίσταται (μέσα στο αρχικό μήνυμα διευθύνσεων ISUP [29] ή στο μήνυμα εγκατάστασης DSS1 [30], αντίστοιχα) για να διαβιβάσει τις πληροφορίες ελέγχου του LI. Αυτές οι πληροφορίες μεταφέρονται διαφανώς και παραδίδονται στον απομακρυσμένο χρήστη LEMF.
Για να προσδιοριστούν οι παραδοθείσες πληροφορίες, συμπεριλαμβανομένου του συσχετισμού των κλήσεων παράδοσης με τις εγγραφές IRI, οι παράμετροι 1 έως 3 και 5 θα πρέπει να συμπεριληφθούν στην εγκατάσταση της κλήσης. Οι παράμετροι 6 έως 9 διευκρινίζουν τις ρυθμίσεις των συμπληρωματικών σχετικών πληροφοριών. Άλλες παράμετροι των πρωτοκόλλων ISDN αντιστοιχούν στις κανονικές βασικές κλήσεις.

A/A	Used information element of CC link signalling protocol	Πληροφορίες
1	CLI-Parameter with attribute "network provided"	Παρ. 4.3.3
2	UUS1-parameter	Lawful Interception IDentifier (LIID), παρ. 4.1
3	UUS1-parameter	Communication IDentifier (CID), παρ. 4.1
4	UUS1-parameter	CC Link IDentifier (CCLID), παρ. 4.1
5	UUS1-parameter	Direction indication (communication from/towards target/combined (mono))
6	UUS1-parameter	Bearer capability of target call
7	Closed user group interlock code	Closed user group interlock code
8	Basic Service (BS)	Basic Service (BS) of CC link: 64 kbit/s unrestricted
9	ISDN user part forward call indicators parameter	ISDN user part preference indicator: "ISDN user part required all the way"
10	ISDN user part optional forward call indicators parameter	Connected line identity request parameter: requested

Πίνακας 6: Ορισμός πληροφοριών σηματοδότησης HI3, λεπτομέρειες κωδικοποίησης UUS1

Οι παράμετροι 2, 3 και 4 είναι επίσης παρούσες στις εγγραφές IRI, για το συσχετισμό με τις συνδέσεις CC. Η παράμετρος 5 καθορίζει το τμήμα που μεταφέρεται από μια σύνδεση CC, στην περίπτωση χωριστής μετάδοσης κάθε κατεύθυνσης επικοινωνίας,. Η παράμετρος 6, η βασική υπηρεσία της κλήσης στόχου, μπορεί να χρησιμοποιηθεί από το LEMF για την επεξεργασία του σήματος CC, π.χ. για να εφαρμόσει τις μεθόδους συμπίεσης για τα σήματα ομιλίας, προκειμένου να εξοικονομήσει χώρο αποθήκευσης. Η παράμετρος 7 περιέχει το CUG του LEA. Χρησιμοποιείται προαιρετικά κατά την εγκατάσταση της σύνδεσης CC με το LEA. Η παράμετρος 8, η βασική υπηρεσία της σύνδεσης CC, τίθεται σε κατάσταση "64 kbit/s unrestricted": Όλες οι πληροφορίες των καναλιών Rx και Tx μπορούν να διαβιβαστούν με πλήρη διαφάνεια στο LEA. Ο καθορισμός της ένδειξης ISDN user part εγγυάται ότι οι υπηρεσίες που υποστηρίζουν την παράδοση LI των συνδέσεων CC, είναι διαθέσιμες για την πλήρη διασύνδεση των συνδέσεων CC.

Το LEMF δεν πρέπει να χρησιμοποιήσει την κατάσταση εγρήγορσης (alerting state), κατά την υποδοχή του μηνύματος εγκατάστασης. Θα πρέπει να συνδέσει αμέσως για να ελαχιστοποιήσει τη χρονική καθυστέρηση μέχρι να γίνει το switching μέσω των συνδέσεων CC. Δεν υποστηρίζουν όλα τα δίκτυα μια τέτοια μετάβαση. Κατ'εξαίρεση, μπορεί να είναι απαραίτητο να σταλεί ένα μήνυμα εγρήγορσης πριν από το συνδεδεμένο μήνυμα. Το μέγιστο μήκος της παραμέτρου πληροφοριών χρήστη μπορεί να είναι μεγαλύτερο από το ελάχιστο μήκος των 35 octets, δηλ. το δίκτυο που διαβιβάζει τις συνδέσεις CC θα υποστηρίξει το τυποποιημένο μέγιστο μέγεθος των 131 octets για την παράμετρο UUS1. Η παράμετρος UUS1 δεν μπορεί να απορριφθεί από τις διαδικασίες ETSI ISUP: ο μόνος λόγος που θα επιτραπεί να την απορρίψουν οι διαδικασίες ISUP, θα είναι εάν το μέγιστο μήκος του μηνύματος που μεταφέρει το UUS1 θα ξεπερνιόταν. Με τον καθορισμένο αριθμό των υπηρεσιών που χρησιμοποιούνται για τις συνδέσεις CC, αυτό δεν μπορεί να συμβεί. Τα μηνύματα σηματοδότησης των δύο καναλιών CC (κατάσταση stereo) μεταφέρουν τις ίδιες τιμές παραμέτρων, εκτός από την ένδειξη κατεύθυνσης.

3.3.3 Οι απαιτήσεις ασφάλειας στη διεπαφη HI3

Η διαδικασία της επαλήθευσης πρόσβασης και της πρόσθετης (προαιρετικής) επικύρωσης μεταξύ του MF και του LEMF, δεν θα πρέπει να καθυστερήσουν την εγκατάσταση των CC.

Για την προστασία και την επαλήθευση πρόσβασης της κλήσης παράδοσης CC, οι συμπληρωματικές υπηρεσίες ISDN όπως είναι η CLIP, COLP και CUG θα χρησιμοποιηθούν όταν διατίθενται στο δίκτυο.

Γενικά οποιαδήποτε διαδικασία πιστοποίησης θα υποβληθεί σε επεξεργασία πριν από την ολοκλήρωση της εγκατάσταση των συνδέσεων CC μεταξύ του MF και του LEMF. Εάν αυτό δεν είναι τεχνικά εφικτό η πιστοποίηση μπορεί να υποβληθεί σε επεξεργασία μετά το πέρας της σύνδεσης CC παράλληλα με την υπάρχουσα σύνδεση.

3.3.3.1 Επαλήθευση πρόσβασης LI

Η συμπληρωματική υπηρεσία CLIP θα χρησιμοποιηθεί για να ελέγξει για τη σωστή προέλευση της κλήσης παράδοσης. Κατά τη χρησιμοποίηση του CLIP, η συμπληρωματική υπηρεσία CLIR δεν πρέπει να χρησιμοποιηθεί.

Η συμπληρωματική υπηρεσία COLP θα χρησιμοποιηθεί για να εξασφαλίσει ότι μόνο το τερματικό από την πλευρά του LEA δέχεται τις εισερχόμενες κλήσεις από τη διεπαφή παράδοσης (Handover Interface, HI). Για να εξασφαλιστεί η επαλήθευση πρόσβασης, θα πρέπει να εκτελεσθούν οι ακόλουθοι δύο έλεγχοι:

- έλεγχος της CLIP (Calling-Line Identification Presentation, CLIP) στο LEMF
- έλεγχος της COLP (COnnected-Line identification Presentation, COLP) στη διεπαφή παράδοσης .

Εξαιτίας του γεγονότος ότι ο συνδεδεμένος αριθμός δεν θα μεταφερθεί πάντα από τα σχετικά δίκτυα, θα υπάρξει η δυνατότητα απενεργοποίησης για τον έλεγχο COLP για ένα δεδομένο μέτρο υποκλοπής. Επιπλέον ο έλεγχος COLP θα δεχτεί δύο διαφορετικούς αριθμούς ως σωστούς αριθμούς, δηλ. Ο αριθμός χρήστη και ο αριθμός δίκτυου. Συνήθως, ο αριθμός χρήστη περιέχει μια επέκταση DDI).

3.3.3.2 Προστασία πρόσβασης

Προκειμένου να αποτραπούν οι ελαττωματικές συνδέσεις στο LEA, οι συνδέσεις CC μπορούν να εγκατασταθούν ως κλήσεις CUG.

Σε αυτήν την περίπτωση, πρέπει να χρησιμοποιηθούν οι ακόλουθες ρυθμίσεις των παραμέτρων CUG:

- Εισερχόμενη πρόσβαση: δεν επιτρέπεται
- Εξερχόμενη πρόσβαση: δεν επιτρέπεται
- Εισερχόμενες κλήσεις που φράζονται μέσα σε ένα CUG: όχι
- Εξερχόμενες κλήσεις που φράζονται μέσα σε ένα CUG: ναι

3.3.3.3 Πιστοποίηση

Εκτός από τους ελάχιστους μηχανισμούς επαλήθευσης πρόσβασης που περιγράφονται ανωτέρω, μπορούν επίσης να χρησιμοποιηθούν προαιρετικοί μηχανισμοί πιστοποίησης σύμφωνα με το πρότυπο ISO 9798. Αυτοί οι μηχανισμοί θα χρησιμοποιηθούν μόνο μαζί με τους μηχανισμούς επαλήθευσης και προστασίας πρόσβασης.

3.4 Διαδικασίες LI για τις συμπληρωματικές υπηρεσίες

3.4.1 Γενικά

Γενικά, το LI θα είναι εφικτό για όλες τις συνδέσεις και τις δραστηριότητες στις οποίες υπεισέρχεται ο στόχος. Ο στόχος δεν θα είναι σε θέση να διακρίνει αλλαγές στην προσφερθείσα υπηρεσία. Επίσης δεν θα είναι δυνατό να αποτραπεί η υποκλοπή με την χρησιμοποίηση των συμπληρωματικών υπηρεσιών. Συνεπώς, από την άποψη των συμπληρωματική υπηρεσιών, η κατάσταση των αλληλεπιδράσεων με το LI δεν προκαλεί κανένα αντίκτυπο, δηλ. η συμπεριφορά των συμπληρωματικών υπηρεσιών δεν θα επηρεαστεί από την νόμιμη υποκλοπή.
Ανάλογα με τον τύπο συμπληρωματικής υπηρεσίας, μπορούν να απαιτηθούν πρόσθετες συνδέσεις CC με το LEA, εκτός από τις ήδη υπάρχουσες συνδέσεις CC.
Μέσα στις εγγραφές IRI, η διαβίβαση πρόσθετων συμπληρωματικών συγκεκριμένων στοιχείων υπηρεσιών μπορεί να απαιτηθεί. Οι συμπληρωματικές υπηρεσίες, που ασκούν επίδραση στο LI, όσον αφορά τις συνδέσεις των CC ή το περιεχόμενο εγγραφών IRI, παρουσιάζονται στον πίνακα 7. Ο πίνακας, που είναι βασισμένος στις υπηρεσίες UMTS, παρουσιάζει τις υπηρεσίες που έχουν τυποποιηθεί. Οι μελλοντικές υπηρεσίες θα πρέπει να ακολουθήσουν τις ίδιες αρχές. Ο συντονισμός του χειρισμού των νέων υπηρεσιών πρέπει να εκτελεσθεί μέσω του 3GPP SA WG3-LI.

Η γενική αρχή είναι, ότι το LI πραγματοποιείται βάσει μιας ταυτότητας, δηλ. ενός αριθμού καταλόγου. Μόνο οι αριθμοί που είναι γνωστοί στους χειριστές (NO/AN/SP), και για τους οποίους το LI έχει ενεργοποιηθεί με τον τυποποιημένο τρόπο, μπορούν να παρεμποδιστούν. Καμία τυποποιημένη λειτουργία δεν είναι διαθέσιμη ακόμα, που θα επέτρεπε σε ένα SCF να ζητήσει από το SSF την επίκληση του LI για μια κλήση.

Οι πρόσθετες συνδέσεις CC απαιτούνται μόνο εάν ο στόχος είναι ο εξυπηρετούμενος χρήστης. Οι εγγραφές IRI μπορούν επίσης να μεταφέρουν δεδομένα από άλλα συμβαλλόμενα μέρη που είναι εξυπηρετούμενοι χρήστες.

Οι προδιαγραφές για τις αλληλεπιδράσεις των συμπληρωματικών υπηρεσιών παραμένουν όσο το δυνατόν περισσότερο ανεξάρτητες από τις λεπτομέρειες των χρησιμοποιημένων πρωτοκόλλων σηματοδότησης. Τα συσχετιζόμενα γεγονότα των υπηρεσιών επομένως περιγράφονται με γενικότερους όρους και όχι χρησιμοποιώντας μηνύματα ή παραμέτρους που εξαρτώνται από το πρωτόκολλο.

Οι αλληλεπιδράσεις με τις υπηρεσίες της ίδιας οικογένειας, όπως οι υπηρεσίες εκτροπής κλήσης (call diversion), ορίζονται σύμφωνα με το LI, εάν η συμπεριφορά των ανεξάρτητων υπηρεσιών είναι η ίδια.

Οι υπηρεσίες, που δεν είναι μέρος του πίνακα 7, δεν απαιτούν την παραγωγή πληροφοριών LI. Δεν παράγονται και δεν τροποποιούνται συνδέσεις CC και καμία συγκεκριμένη πληροφορία για την υπηρεσία δεν είναι παρούσα στις εγγραφές IRI. Επομένως αυτές οι υπηρεσίες δεν ασκούν καμία επίδραση (no impact) στο LI, δηλαδή δεν απαιτείται καμία πρόσθετη λειτουργία για το LI. Εντούτοις, μέσα στο IIF, μπορεί να απαιτηθούν κάποιες λειτουργίες για να εξασφαλιστεί ότι η συμπεριφορά υπηρεσιών δεν θα επηρεαστεί από το LI. Η αρχή της μηδενικής επίδρασης (no impact) δεν ισχύει αυτόματα για τις νέες υπηρεσίες. Κάθε νέα υπηρεσία πρέπει να ελεγχθεί για την επίδρασή της πάνω στο LI.

Συμπλ. Υπηρ.	Συντομογραφία	Συνδέσεις CC: επιπρόσθετες κλήσεις, επίδραση	Στοιχεία IRI που σχετίζονται με την υπηρεσία
Call Waiting	CW	CC links for active or all calls (option A/B)	Target: call waiting indication, calling party address other party: generic notification indicator
Call Hold	HOLD	CC links for active or all calls (option A/B)	Target: call hold indication other party: generic notification indicator
Call Retrieve	RETRIEVE	CC links for active or all calls (option A/B)	Target: call retrieve indication other party: generic notification indicator
Explicit Call Transfer	ECT	Before transfer: see HOLD After transfer: LI may or may not be stopped	Target: components of Facility IE other party: generic notification indicator
Subaddressing	SUB	No impact on CC links	Subaddress IE, as available (calling, called, ...)
Calling Line Identification Presentation	CLIP	No impact on CC links	CLI parameter: part of originating-Party information
Calling Line Identification Restriction	CLIR	No impact on CC links	Restriction indicator is part of CLI parameter
Connected Line Identification Presentation	COLP	No impact on CC links	COL parameter: part of terminating-Party information
Connected Line Identification Restriction	COLR	No impact on CC links	Restriction indicator is part of COL parameter
Closed User Group	CUG	No impact on CC links	CUG interlock code
Multi Party Conference	MPTY	Initially: held and active calls see HOLD Conf.: T_X: signal from target; Rx call sum signal CC links depending on option A/B	Target: components of Facility IE other party: generic notification indicator
Call Forwarding Unconditional; see note	CFU	One CC link for each call, which is forwarded by the target Forwarding by other parties: no impact	if redirecting no. = target DN: not included Other party (call to target is a forwarded call) Other party (call from target gets forwarded)
Call Forwarding No Reply; see note	CFNRy	1) basic call with standards CC links, released after time-out (incl. CC links) 2) forwarding: same as CFU	1) basic call, released after time-out, standard IRI 2) forwarding: same parameters as for CFU
Call Forwarding Not Reachable; see note	CFNRc	See CFU	See CFU
Call Forwarding Busy; see note	CFB	Network determined user busy: see CFU User determined user busy: see CFNR	Network determined user busy: see CFU user determined user busy: see CFNR

Συμπλ. Υπηρ.	Συντομογραφία	Συνδέσεις CC: επιπρόσθετες κλήσεις, επίδραση	Στοιχεία IRI που σχετίζονται με την υπηρεσία
Call Deflection	CD	See CFNR	See CFNR
User-to-User Signalling 1, 2, 3	UUS	No impact on CC links	User-to-user information, more data IE (part of HI2 information). In ETSI HI3 was used. Optionally, ETSI's HI3 interface for UUS may be maintained for backwards compatibility reasons.
Fallback procedure (not a supplemen-tary service)	FB	No impact on CC links	Target or other party: new basic service IE

Πίνακας 7: Συμπληρωματικές υπηρεσία με επίδραση στις CC συνδέσεις LI ή στο περιεχόμενο εγγραφών IRI

3.4.2 Επίδραση συνδέσεων CC

Η στήλη "Συνδέσεις CC: επιπρόσθετες κλήσεις, επίδραση" (δείτε τον πίνακα 4.7) καθορίζει:

- εάν για τη σχετική υπηρεσία, θα εγκατασταθούν CC συνδέσεις, επιπρόσθετα από τις CC συνδέσεις της βασικής κλήσης
- εάν υπάρχει επίδραση μεταξύ των κλήσεων που ήδη υπάρχουν, παραδείγματος χάριν με την αποσύνδεση της ροής πληροφοριών τους.

Η επίδραση των CC συνδέσεων αφορά πάντα τις ενέργειες ενός στόχου που είναι ο εξυπηρετούμενος χρήστης. Η κλήση υπηρεσιών από άλλα συμβαλλόμενα μέρη δεν ασκούν καμία επίδραση στις συνδέσεις CC.

3.4.3 Επίδραση IRI, Γενική αρχή για την αποστολή εγγραφών IRI.

Η στήλη " Στοιχεία IRI που σχετίζονται με την υπηρεσία " (δείτε τον πίνακα 7) διευκρινίζει τις παραμέτρους που μπορούν να μεταδοθούν στο LEA μέσα σε εγγραφές IRI. Διάφορες υπηρεσίες, διαφοροποιούνται εάν ο στόχος ή το άλλο συμβαλλόμενο μέρος είναι ο εξυπηρετούμενος χρήστης. Ο πίνακας διευκρινίζει ποιες παράμετροι ισχύουν σε γενικές γραμμές. Δηλαδή, αυτές οι παράμετροι στέλνονται κανονικά στο LEA αμέσως μόλις είναι

διαθέσιμες από τις διαδικασίες του πρωτοκόλλου της υπηρεσίας. Σε πολλές περιπτώσεις θα παραχθούν επιπρόσθετες εγγραφές IRI-CONTINUE σε σχέση με αυτές μιας βασικής κλήσης.

Εντούτοις δεν είναι απαραίτητο να σταλεί αμέσως κάθε γεγονός σηματοδότησης, που είναι σχετικό με την υπηρεσία, μέσα σε μια μεμονωμένη εγγραφή. Εξαιρέσεις μπορούν να υπάρξουν, όπου διάφορα γεγονότα συμπεριλαμβάνονται σε μια εγγραφή, ακόμα κι αν αυτό θα οδηγούσε σε κάποια καθυστέρηση της αναφοράς ενός γεγονότος (αυτό μπορεί να εξαρτάται από την υλοποίηση). Κάθε εγγραφή θα περιέχει όλες τις πληροφορίες, οι οποίες απαιτούνται από το LEA για να επιτρέψουν την ερμηνεία μιας ενέργειας. Για παράδειγμα: η ένδειξη της κλήσης που προωθείται από το στόχο θα περιλαμβάνει τον αριθμό που γίνεται η προώθηση και την ένδειξη του τύπου προώθησης μέσα στην ίδια εγγραφή. Το πλήρες σύνολο παραμέτρων, που ισχύουν για το IRI, διευκρινίζεται στην πρόταση 3.2.3 (δείτε τον πίνακα 5).

Εάν κατά τη διάρκεια των διαδικασιών που περιλαμβάνουν τις συμπληρωματικές υπηρεσίες, γίνουν διαθέσιμες οι παράμετροι πρωτοκόλλου που παρατίθενται στον πίνακα 4.5, τότε θα συμπεριληφθούν στις εγγραφές IRI.

Τα δεδομένα IRI δεν αποθηκεύονται από το IIF ή το MF με σκοπό την αποθήκευση πληροφοριών σχετικά με την κλήση ή τη διαμόρφωση της κλήσης. Το LEMF (ηλεκτρονικά) ή ο πράκτορας του LEA (χειροκίνητα) θα είναι πάντα σε θέση να ανακαλύψουν το σχετικό ιστορικό στη διαμόρφωση της κλήσης, στην έκταση που δίνεται από τις διαθέσιμες πληροφορίες του πρωτόκολλου σηματοδότησης, μέσα στο δίκτυο τηλεπικοινωνιών.

Οι επικλήσεις υπηρεσιών χρειάζεται να αναφερθούν μόνο σε περίπτωση πραγματοποίησης επιτυχών επικλήσεων. Μία εγγραφή IRI, που περιέχει το στοιχείο που επικαλείται και που ενδεχομένως συμπεριλαμβάνει πρόσθετες παραμέτρους από το στοιχείο επιστροφής αποτελέσματος, είναι ικανοποιητική.

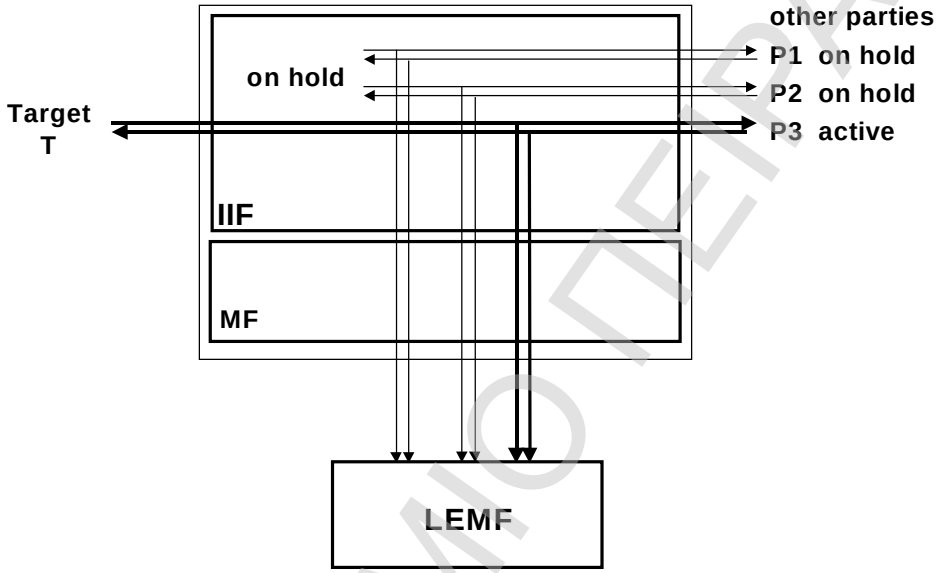
3.4.4.1 Συνδέσεις CC για ενεργές και μη ενεργές κλήσεις (επιλογή A)

Για κάθε κλήση, ενεργή ή όχι, πρέπει να παρέχονται ξεχωριστές συνδέσεις CC. Κάτι τέτοιο εγγυάται ότι:

- οι αλλαγές στη διαμόρφωση κλήσης του στόχου απεικονίζονται αμέσως, χωρίς καθυστέρηση, στο LEMF

- το σήμα από τα συμβαλλόμενα μέρη μπορεί να υποκλαπεί ακόμα.

Αποτελεί μια επιλογή δικτύου το εάν η κατεύθυνση επικοινωνίας μιας μη ενεργής κλήσης, που φέρει ένα σήμα από το άλλο συμβαλλόμενο μέρος, δρομολογείται στο LEMF ή διακόπτεται.

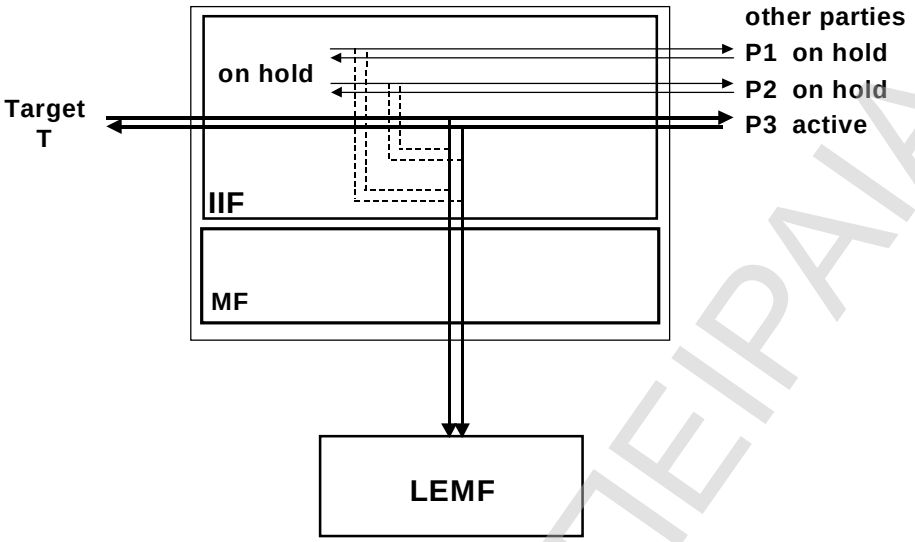


Εικόνα 2: Σύνδεση CC, επιλογή A

3.4.4.2 Επαναχρησιμοποίηση των συνδέσεων CC για τις ενεργές κλήσεις (επιλογή B).

Οι συνδέσεις CC χρησιμοποιούνται μόνο για τις κλήσεις που είναι ενεργές στη φάση επικοινωνίας. Αλλαγές στη διαμόρφωση κλήσης δεν μπορούν να απεικονιστούν στο LEMF αμέσως, επειδή απαιτείται η μεταστροφή (switching) στο IIF/MF, και το σήμα από το κρατημένο συμβαλλόμενο μέρος δεν είναι διαθέσιμο.

Κάθε φορά που ένα άλλο σκέλος κλήσης στόχος χρησιμοποιεί μια υπάρχουσα σύνδεση CC, θα σταλεί μια εγγραφή IRI-CONTINUE με το σωστό CID και CCLID. Ακόμα και όταν χρησιμοποιείται η επιλογή B, περισσότερες από μια συνδέσεις CC μπορούν να απαιτηθούν ταυτόχρονα.



Εικόνα 3: Σύνδεση CC, επιλογή B

3.4.5 Ελεγχόμενη είσοδος από τον συνδρομητή (Subscriber Controlled Input, SCI): Ενεργοποίηση/απενεργοποίηση/ερώτηση των υπηρεσιών.

Για τις διαδικασίες χρηστών για τον έλεγχο των συμπληρωματικών υπηρεσιών (ενεργοποίηση/απενεργοποίηση/ερώτηση), ορίζεται ένας ειδικός τύπος εγγραφής IRI (εγγραφή IRI-REPORT) για να διαβιβάσει τις απαραίτητες πληροφορίες.

Η εγγραφή IRI-REPORT θα περιλαμβάνει έναν δείκτη που ενημερώνει εάν η αίτηση του στόχου έχει επεξεργαστεί με επιτυχία ή όχι.

3.5 Λεπτομερείς διαδικασίες για τις συμπληρωματικές υπηρεσίες

3.5.1 Υπηρεσίες γνωστοποίησης των δαπανών (Advice of Charge, AOC)

Καμία επίδραση. Οι υπηρεσίες γνωστοποίησης των δαπανών δεν συμπεριλαμβάνονται στις εγγραφές IRI.

3.5.2 Αναμονή κλήσης (CW)

3.5.2.1 Αναμονή κλήσης στο στόχο: Συνδέσεις CC

Σε περίπτωση της επιλογής A "CC links for all calls", μια σύνδεση CC εγκαθίσταται για την κλήση αναμονής, χρησιμοποιώντας τις τυποποιημένες διαδικασίες για τις κλήσεις τερματισμού. Σε περίπτωση της επιλογής B "CC links for active calls", καμία σύνδεση CC δεν εγκαθίσταται για την κλήση αναμονής, απλώς αντιμετωπίζεται όπως μια κρατημένη κλήση.
Όσον αφορά τις συνδέσεις CC, ισχύουν οι ίδιες διαμορφώσεις όπως για τη Call Hold.

3.5.2.2 Αναμονή κλήσης: IRI records.

3.5.2.2 .1 Ο στόχος είναι εξυπηρετούμενος χρήστης.

Εάν η αναμονή κλήσης επικληθεί στην πρόσβαση του στόχου από ένα άλλο συμβαλλόμενο μέρος τότε: η εγγραφή IRI-BEGIN ή μια ακόλουθη IRI-CONTINUE για την κλήση αναμονής περιέχει την παράμετρο LI *call waiting indication*.

3.5.2.2 .2 Το άλλο συμβαλλόμενο μέρος είναι εξυπηρετούμενος χρήστης

Εάν η αναμονή κλήσης καλείται στην πρόσβαση του άλλου καλούμενου συμβαλλόμενου μέρους: εάν ληφθεί ένα *CW notification* από τον κόμβο δρομολόγησης του στόχου, θα περιληφθεί μέσα σε μια εγγραφή IRI-CONTINUE. Αυτή θα είναι μια χωριστή εγγραφή, ή η επόμενη εγγραφή της ακολουθίας της βασικής κλήσης.

3.5.3 Κράτηση/Ανάκτηση κλήσης

3.5.3.1 Συνδέσεις CC για τις ενεργές και μη ενεργές κλήσεις (επιλογή A).

Εάν μια ενεργός κλήση τίθεται σε κράτηση, οι συνδέσεις CC θα μείνουν άθικτες. Εάν ο στόχος εγκαταστήσει μια νέα κλήση, ενώ μια κλήση είναι σε κράτηση, αυτή η κλήση αντιμετωπίζεται όπως μια κανονική κλήση, δηλ. καθιερώνεται μια νέα διαμόρφωση LI (συνδέσεις CC, εγγραφές IRI).

3.5.3.2 Επαναχρησιμοποίηση των συνδέσεων CC για τις ενεργές κλήσεις (επιλογή B)

Εάν μια ενεργός κλήση τίθεται σε κράτηση, οι CC συνδέσεις της δεν θα αποσυνδεθούν αμέσως. Υπάρχει η επιλογή, το σήμα από το κρατημένο συμβαλλόμενο μέρος να μην δρομολογείται στο LEMF.

Εάν ο στόχος οργανώσει μια νέα κλήση ή ανακτήσει μια προηγουμένως κρατημένη κλήση, ενώ μια κλήση στόχος στην οποία ανήκουν ακόμα συνδέσεις CC, είναι σε κράτηση, αυτές οι συνδέσεις CC θα χρησιμοποιηθούν για τα σήματα της νέας ενεργού κλήσης.

3.5.3.3 Εγγραφές IRI

3.5.3.3 .1 Επίκληση Κράτησης/Ανάκτησης κλήσης από το στόχο

Μια εγγραφή IRI-CONTINUE με την παράμετρο ένδειξης κράτησης ή ανάκτησης, αντίστοιχα, θα σταλεί.

3.5.3.3.2 Επίκληση Κράτησης/Ανάκτησης κλήσης από άλλα συμβαλλόμενα μέρη

Μια εγγραφή IRI-CONTINUE με μια ειδοποίηση κράτησης/ανάκτησης κλήσης θα αποσταλεί εάν έχει ληφθεί από την οντότητα του πρωτοκόλλου σηματοδότησης της κλήσης στόχου.

3.5.4 Ρητή μεταφορά κλήσης (Explicit Call Transfer, ECT).

3.5.4.1 Ρητή μεταφορά κλήσης, σύνδεση CC.

Κατά τη διάρκεια της φάσης προετοιμασίας μιας μεταφοράς, ισχύουν οι διαδικασίες για την κράτηση/ανάκτηση κλήσης. Εάν ο εξυπηρετούμενος χρήστης είναι ο στόχος, η αρχική κλήση της απελευθερώνεται. Αυτό τερματίζει επίσης τη σύνδεση CC και προκαλεί την αποστολή μιας εγγραφής IRI-END. Μετά από τη μεταφορά, υπάρχουν δύο επιλογές:

1) Για τη μεταφερμένη κλήση, οι συνδέσεις CC και οι εγγραφές IRI θα παραχθούν, σε γενικές γραμμές όπως για μια προωθημένη κλήση *(παρόμοια με τις διαδικασίες στην 4.5.12.1 .1, περίπτωση β))*

2) Η μεταφερμένη κλήση δεν θα υποκλαπεί.

3.5.4.2Ρητή μεταφορά κλήσης, εγγραφές IRI.

Επιπρόσθετα με τις σχετικές εγγραφές για την βασική κλήση ή την κλήση σε κράτηση/ανακτηση/αναμονή, κατά τη διάρκεια του επαναδιαμόρφωση της κλήσης, αποστέλλονται πληροφορίες ECT, στην πρόσβαση του στόχου στο LEMF, μέσα σε εγγραφές IRI-CONTINUE.
Όταν ο στόχος εγκαταλείπει την κλήση μετά την μεταφορά, αποστέλλεται μια εγγραφή IRI-END και η δοσοληψία του LI τερματίζεται.

3.5.5 Calling Line Identification Presentation (CLIP), Εγγραφές IRI

3.5.5.1 Κλήση που προέρχεται από το στόχο (ο στόχος είναι εξυπηρετούμενος χρήστης)

Η παράμετρος CLI ενός στόχου συμπεριλαμβάνεται ως παράμετρος συμπληρωματικής υπηρεσίας στις εγγραφές IRI.

3.5.5.2 Κλήση που τερματίζεται στο στόχο, (το άλλο συμβαλλόμενο μέρος είναι εξυπηρετούμενος χρήστης)

Το CLI που στέλνεται από το άλλο συμβαλλόμενο μέρος συμπεριλαμβάνεται στην εγγραφή IRI-BEGIN ανεξάρτητα από μια ένδειξη περιορισμού (πληροφορία *originating-Party*). Ένας λαμβανόμενος δεύτερος αριθμός (περίπτωση δύο, επιλογή παράδοσης αριθμού) συμπεριλαμβάνεται στην εγγραφή IRI ως πληροφορία συμπληρωματικών υπηρεσιών (παράμετρος Generic Number).

3.5.6 Calling Line Identification Restriction (CLIR)

Προς χρήση από το LI. Ο περιορισμός αγνοείται, αλλά αντιγράφεται μέσα στην παράμετρο CLI στην εγγραφή IRI.

3.5.7 COnnected Line identification Presentation (COLP)

3.5.7.1 Τερματισμός κλήσης στο στόχο (ο στόχος είναι εξυπηρετούμενος χρήστης)

Μια παράμετρος συνδεδεμένου αριθμού που παραλαμβάνεται από το στόχο θα περιληφθεί σε μια εγγραφή IRI (πληροφορία terminating-Party).

3.5.7.2 Κλήση προερχόμενη από το στόχο. (το άλλο συμβαλλόμενο μέρος είναι εξυπηρετούμενος χρήστης)

Εάν είναι διαθέσιμη, μια παράμετρος συνδεδεμένου αριθμού όπως παραλαμβάνεται από το άλλο (τερματικό) συμβαλλόμενο μέρος, θα περιληφθεί σε μια εγγραφή IRI (πληροφορία terminating-Party). Οποιοσδήποτε πρόσθετος αριθμός, π.χ. ένας Γενικός Αριθμός, θα περιληφθεί επίσης στην εγγραφή IRI.

3.5.8 COnnected Line identification Restriction (COLR)

Προς χρήση από το LI. Ο περιορισμός αγνοείται, αλλά αντιγράφεται μέσα στην παράμετρο COL στην εγγραφή IRI.

3.5.9 Κλειστή ομάδα χρηστών (Closed User Group, CUG).

Σε περίπτωση κλήσης CUG, ο κώδικας interlock της κλειστής ομάδας χρηστών θα περιληφθεί σε ένα IRI.

3.5.10 Completion of Call to Busy Subscriber (CCBS)

Καμία επίδραση.Η πρώτη κλήση, η οποία συναντά έναν τερματικό busy συνδρομητή, και απελευθερώνεται στη συνέχεια, αντιμετωπίζεται όπως μια τυποποιημένη busy κλήση, χωρίς σχετικές CCBS πληροφορίες IRI.

Οι διαδικασίες για το CCBS, μέχρι την έναρξη μιας νέας προσπάθειας κλήσης από τον εξυπηρετούμενο χρήστη στον τερματικό χρήστη, συμπεριλαμβανομένης της ανάκλησης CCBS, δεν είναι υπαγόμενες στο LI.

3.5.11 Κλήση Multi Party (Multi ParTY, MPTY).

Η συνδιάσκεψη MPTY προέρχεται από μια διαμόρφωση με δύο κλήσεις (μια ενεργή και μια που είναι σε κράτηση). Κατά την ένωση των κλήσεων σε μια συνδιάσκεψη, οι συνδέσεις CC, που έχουν φέρει τα σήματα της ενεργού κλήσης στόχου, χρησιμοποιούνται για να διαβιβάσουν τα σήματα της συνδιάσκεψης. Δηλαδή, η κλήση Rx περιέχει το συνολικό σήμα της συνδιάσκεψης και η κλήση Tx περιέχει το σήμα από τον στόχο.
Το δεύτερο σύνολο συνδέσεων CC, για την προηγουμένη κρατημένη κλήση, μένει άθικτο. Εάν η συνδιάσκεψη αποδεσμεύεται και επανεγκαθίσταται η αρχική κατάσταση (μια κρατημένη και μια ενεργή κλήση), οι απαραίτητες συνδέσεις CC είναι ακόμα διαθέσιμες. εάν ο στόχος είναι παθητικό συμβαλλόμενο μέρος της συνδιάσκεψης τότε δεν υπάρχει καμία επίδραση στις συνδέσεις CC.

3.5.11.2 Εγγραφές IRI.

Για τα γεγονότα, που ορίζουν την έναρξη και το τέλος της συνδιάσκεψης MPTY, παράγονται εγγραφές IRI.

3.5.12 Υπηρεσίες εκτροπής (DIVersion Services, DIV).

Οι κλήσεις σε έναν στόχο, με τον αριθμό συμβαλλόμενων μερών (party number) να είναι ίσος με τον DN του στόχου υποκλοπής, υποκλέπτονται, δηλαδή οι συνδέσεις CC εγκαθίστανται και οι εγγραφές αρχεία IRI στέλνονται στο LEA. Αυτό ισχύει για όλα τα είδη προώθησης κλήσεων.
Για τις κλήσεις που προωθούνται από το άλλο συμβαλλόμενο μέρος (που καλεί ή καλείται), οι διαθέσιμες πληροφορίες, που είναι σχετικές με την εκτροπή, στέλνονται στο LEA.

3.5.12.1 Εκτροπή κλήσης από το στόχο.

3.5.12.1 .1 Εκτροπή κλήσης από το στόχο, συνδέσεις CC

Προκειμένου να γίνει η διαχείριση των υπηρεσιών εκτροπής κλήσης, όσο το δυνατόν περισσότερο, με την εφαρμογή κοινών διαδικασιών, έχουμε τις ακόλουθες δύο περιπτώσεις:

α) Call Forwarding Unconditional (CFU), Call Forwarding Busy (NDUB):

Σε αυτές τις περιπτώσεις, η προώθηση καθορίζεται, πριν γίνει η κατάληψη στην πρόσβαση στόχου. Οι συνδέσεις CC εγκαθίστανται αμέσως για την προωθημένη κλήση. Άλλες παραλλαγές της προώθησης κλήσης αντιμετωπίζονται με τον ίδιο τρόπο.

β) Call Forwarding No Reply, Call Forwarding Busy (UDUB) και Εκτροπή κλήσης.

Αρχικά, εγκαθίσταται η κλήση στόχος και η κλήση υποκλέπτεται όπως μια βασική κλήση.

Κατά την πραγματοποίηση της προώθησης (π.χ. μετά την λήξη του μετρητή CFNR), η αρχική κλήση απελευθερώνεται. Αυτό μπορεί να προκαλέσει επίσης μια απελευθέρωση των συνδέσεων CC. Σε αυτήν την περίπτωση πρέπει να ισχύσουν δύο προαιρετικοί χειρισμοί εγγραφών IRI:

1) Για την αρχική κλήση στέλνεται μια εγγραφή IRI-END. Για την προωθημένη κλήση μια νέα διαδικασία εγκατάστασης, συμπεριλαμβανομένης της νέας συναλλαγής LI, μπορεί να πραγματοποιηθεί με το νέο σύνολο εγγραφών IRI (αρχίζοντας από την εγγραφή IRI-BEGIN που στέλνεται στο LEA).

2) Για την προωθημένη κλήση παράγεται η εγγραφή IRI-CONTINUE και στέλνεται σε ένα LEA, επισημαίνοντας έτσι την επίκληση του CFNR.

Σε περίπτωση πολλαπλής προώθησης, μια κλήση μπορεί να υποκλαπεί αρκετές φορές, εάν διάφορα συμβαλλόμενα μέρη είναι στόχοι. Εξετάζοντας το μέγιστο αριθμό εκτροπών για μια κλήση των πέντε (5 είναι το συνιστώμενο όριο στο 3GPP), μια κλήση μπορεί να υποκλαπεί 7 φορές, από το ίδιο ή διαφορετικό LEA. Σε γενικές γραμμές, αυτές οι διαδικασίες είναι ανεξάρτητες μεταξύ τους.

3.5.12.1 .2 Εκτροπή κλήσης από το στόχο, εγγραφές IRI

Δείτε το 3.2.2.3, περίπτωση 2, που είναι σχετική με τις πληροφορίες του στόχου, και την περίπτωση 3, που είναι σχετική με τις πληροφορίες προώθησης. Όπως παραπάνω για τις συνδέσεις CC, οι τύποι εκτροπής διαφοροποιούνται:

Για την περίπτωση εκτροπών α και b2, το IRI είναι μέρος μιας συναλλαγής IRI-BEGIN/CONTINUE/END. Για τις εκτροπές περίπτωσης b1, μια πρώτη συναλλαγή ενημερώνει για το τμήμα κλήσης, έως ότου επικληθεί η εκτροπή που αντιστοιχεί σε μια βασική πρόωρα

απελευθερωμένη κλήση, και μια δεύτερη συναλλαγή ενημερώνει για το τμήμα κλήσης, όταν επικαλείται η εκτροπή (αντιστοιχεί στην περίπτωση α).

3.5.12.2 Προωθημένη κλήση που τερματίζεται στο στόχο

Η σύνδεση CC αντιμετωπίζεται με τον τυποποιημένο τρόπο. Η εγγραφή IRI-BEGIN περιέχει τις διαθέσιμες πληροφορίες εκτροπής κλήσης, περίπτωση 1 του 3.2.2.3.

3.5.12.3 Κλήση από το στόχο που προωθείται

Η σύνδεση CC αντιμετωπίζεται με τον τυποποιημένο τρόπο. Η εγγραφή IRI-BEGIN, και πιθανότατα και η IRI-CONTINUE, περιέχει τις διαθέσιμες πληροφορίες εκτροπής κλήσης, περίπτωση 3 του 3.2.2.3.

3.5.13 Παραλλαγές των υπηρεσιών εκτροπής κλήσης.

Οι παραλλαγές των ανωτέρω «τυποποιημένων» υπηρεσιών εκτροπής αντιμετωπίζονται με τον ίδιο τρόπο όπως η αντίστοιχη «τυποποιημένη» υπηρεσία εκτροπής.

3.5.14 Υποδιευθυνσιοδοτηση (SUBaddressing, SUB)

Οι διαφορετικοί τύποι των στοιχείων πληροφοριών υποδιευθυνσιοδότησης είναι μέρος των εγγραφών IRI, σε όλες τις περιπτώσεις βασικών και συμπληρωματικών υπηρεσιών όπου είναι παρόντα.

4.5.15 Σηματοδότηση από Χρήστη-σε-Χρήστη (User-to-User Signalling, UUS).

Οι παράμετροι των υπηρεσιών UUS1, UUS2 και UUS3 θα αναφερθούν ως HI2

3.5.16 Incoming Call Barring (ICB).

Καμία επίδραση.

α) Περίπτωση τερματικής κλήσης σε έναν στόχο με το ICB ενεργό:

Γενικά η συνθήκη περιορισμού ενός στόχου ανιχνεύεται προτού να καθοριστεί η πρόσβαση στόχου και έτσι παράγεται μια εγγραφή IRI-REPORT .

β) Περίπτωση που ο στόχος καλεί ένα συμβαλλόμενο μέρος με το ICB ενεργό:
Σε γενικές γραμμές, μία εγγραφή IRI-BEGIN έχει σταλεί ήδη και οι συνδέσεις CC έχουν εγκατασταθεί. Συνεπώς, παράγεται μια συνηθισμένη εγγραφή IRI-END.

3.5.17 Outgoing Call Barring (OCB)

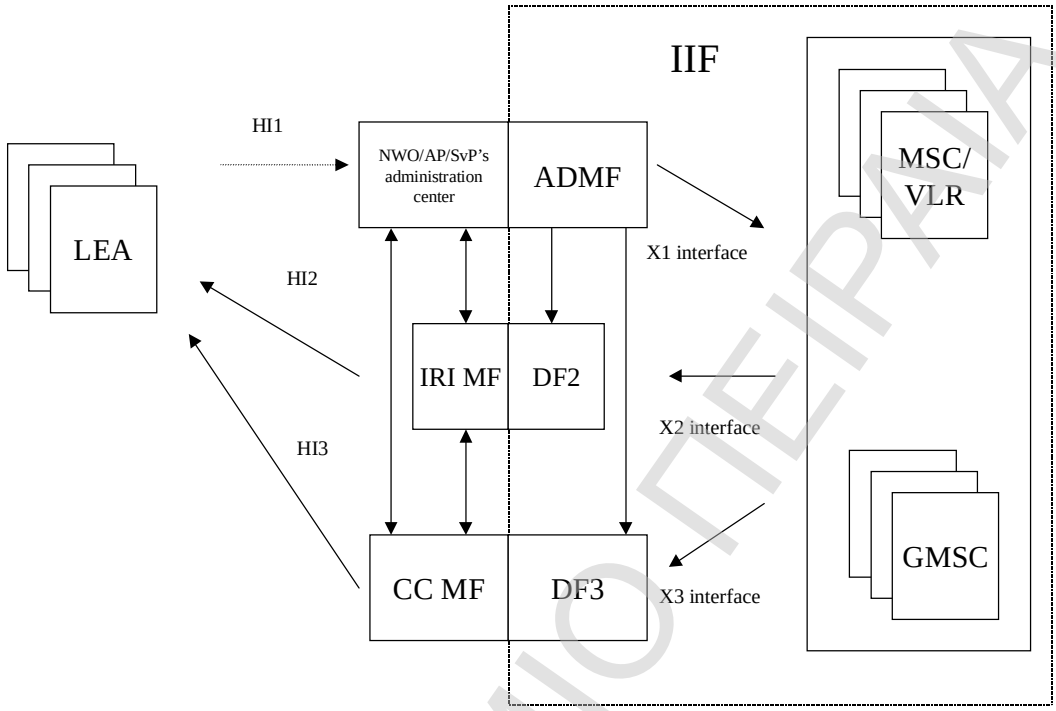
Καμία επίδραση.Για μια εμποδισμένη κλήση, μια τυπική εγγραφή μπορεί να δημιουργηθεί. Ο τύπος της και το περιεχόμενο της εξαρτώνται στο σημείο της κλήσης, που έχει αποδεσμευτεί λόγω των περιορισμών OCB.

3.5.18 Τόνοι και Αναγγελίες

Καμία επίδραση.Εάν οι κανονικές διαδικασίες, ανάλογα με την κατάσταση της κλήσης, έχουν ως αποτέλεσμα την αποστολή του σήματος τόνου ή αναγγελίας στο κανάλι Rx της σύνδεσης CC, τότε αυτό θα μεταβιβαστεί ως CC.

3.6 Λειτουργική αρχιτεκτονική

Η ακόλουθη εικόνα περιέχει τη διαμόρφωση-πρότυπο για τη νόμιμη παρεμπόδιση. Υπάρχει μια λειτουργία διαχείρισης (Administration Function, ADMF) στο δίκτυο. Μαζί με τις λειτουργίες παράδοσης χρησιμοποιείται για να κρύψει από τον διακομιστή 3G MSC και τον 3G GMSC, το γεγονός ότι μπορεί να υπάρχουν πολλαπλές ενεργοποιήσεις από τα διαφορετικά LEA (Law Enforcement Agencies, LEA) στον ίδιο στόχο.



Εικόνα 4: Διαμόρφωση-πρότυπο για Circuit switched

Η διαμόρφωση-πρότυπο αποτελεί μια λογική αναπαράσταση των οντοτήτων που περιλαμβάνονται στη νόμιμη υποκλοπή και δεν υποχρεώνει την ύπαρξη ξεχωριστών φυσικών οντοτήτων. Αυτό επιτρέπει μεγαλύτερο επίπεδο ενσωμάτωσης.

Μια κλήση θα μπορούσε να υποκλαπεί βάσει διαφορετικών ταυτοτήτων (MSISDN, IMSI, IMEI) του ίδιου στόχου. Η υποκλοπή που είναι βασισμένη στο IMEI θα μπορούσε να οδηγήσει σε μια καθυστέρηση στην έναρξη της υποκλοπής στην αρχή μιας κλήσης. Η υποκλοπή γεγονότων που δεν σχετίζονται με την κλήση, δεν είναι δυνατή. Για την παράδοση των CC και του IRI, ο διακομιστής 3G MSC ή ο 3G GMSC παρέχει τον αριθμό συσχετισμού και την ταυτότητα στόχου στα DF2 και DF3 και χρησιμοποιείται εκεί προκειμένου να επιλεχτεί το διαφορετικό LEA όπου το προϊόν θα παραδοθεί.

6.2 Μηχανισμοί εμπιστευτικότητας

Εάν η τοπική πολιτική στο P-CSCF απαιτήσει τη χρήση συγκεκριμένου μηχανισμού προστασίας εμπιστευτικότητας IMS μεταξύ του UE και του P-CSCF, το IPsec ESP όπως ορίζεται στο RFC 2406 [13] θα παράσχει την προστασία εμπιστευτικότητας της σηματοδότησης SIP μεταξύ του UE και του P-CSCF. Αυτό θα έχει σαν αποτέλεσμα την προστασία όλων των μηνυμάτων σηματοδότησης SIP σε επίπεδο IP. Επίσης θα πρέπει να τεθούν υπόψιν και οι γενικές έννοιες IPSec ESP στην διαχείριση της πολιτικής ασφάλειας, τους συσχετισμούς ασφάλειας και την επεξεργασία κυκλοφορίας IP όπως περιγράφεται στο RFC 2401 [14]. Η εμπιστευτικότητα ESP θα εφαρμοστεί σε κατάσταση μεταφοράς (transport mode) μεταξύ του UE και του P-CSCF.

Ως συνέπεια μιας πιστοποιημένης διαδικασία εγγραφής, θα καθιερωθούν δύο ζευγάρια από ομοιοκατευθυνόμενα (uni-directional) SAs μεταξύ του UE και του P-CSCF.

Το ένα ζευγάρι SA είναι για την κυκλοφορία μεταξύ μιας θύρας πελάτη στο UE και μιας θύρας διακομιστή στο P-CSCF. Το άλλο SA είναι για την κυκλοφορία μεταξύ μιας θύρας πελάτη στο P-CSCF και μιας θύρας διακομιστή στο UE.

Το κλειδί κρυπτογράφησης CK_{ESP} είναι το ίδιο για τα δύο ζευγάρια των ταυτόχρονα καθιερωμένων SA. Το κλειδί κρυπτογράφησης CK_{ESP} λαμβάνεται από το κλειδί CK_{IM} που καθιερώνεται ως συνέπεια της διαδικασίας AKA, χρησιμοποιώντας μια κατάλληλη συνάρτηση επέκτασης κλειδιού.

Η επέκταση κλειδιού κρυπτογράφησης από την πλευρά του χρήστη γίνεται στο UE. Η επέκταση κλειδιού κρυπτογράφησης από την πλευρά του δικτύου γίνεται στο P-CSCF.

6.5 Διαλειτουργικότητα του CSCF με τον μεσολαβητή (proxy) που βρίσκεται σε ένα δίκτυο μη-IMS.

Η σηματοδότηση SIP που προστατεύεται από το TLS, το οποίο ορίζεται στο RFC 3261 [6], μπορεί να χρησιμοποιηθεί για την προστασία της λειτουργικότητας του SIP μεταξύ ενός IMS CSCF με ένα proxy/CSCF που βρίσκεται σε ένα ξένο δίκτυο. Το CSCF μπορεί να ζητήσει τη σύνδεση TLS με ένα ξένο μεσολαβητή με την έκδοση των SIPS: ένα URI σε έναν διακομιστή

DNS που μπορεί να βρεθεί μέσω του μηχανισμού NAPTR/SRV που ορίζεται στο RFC 3263 [23]. Κατά την αποστολή/λήψη του πιστοποιητικού κατά την διάρκεια της φάσης χειραψίας του TLS, το CSCF θα ελέγξει το όνομα στο πιστοποιητικό μέσα στον κατάλογο των «συνεργατών». Η σύνοδος TLS θα μπορεί να αρχικοποιηθεί και από τα δύο δίκτυα. Μια σύνδεση TLS είναι ικανή να μεταφέρει πολλαπλούς διαλόγους SIP.

Η εφαρμογή αυτής της μεθόδου πρόκειται να αποτρέψει τις επιθέσεις σε επίπεδο SIP, αλλά δεν απαγορεύει την εφαρμογή και άλλων μεθόδων ασφάλειας ώστε να ενισχυθεί περαιτέρω η ασφάλεια των IP δικτύων. Αυτό το σημείο ορίζεται στο Annex A του TS 33.210 [5].

Κεφάλαιο 4

Δίκτυα B3G

4.1 Η τεχνολογία B3G

Η σημερινή εξέλιξη των δικτύων κινητών επικοινωνιών ίσως ήταν κάτι πολύ δύσκολο να προβλέψει ή και να φανταστεί κανείς πριν από 20 χρόνια. Σήμερα, η διείσδυση της λεγόμενης «κινητής επικοινωνίας 2ης Γενιάς» (2Γ ή 2G), δηλ. της γνωστής σε όλους μας κινητής τηλεφωνίας φωνής (μόνο), καταγράφει ποσοστά που σε πολλές χώρες ξεπερνούν το 50%, φθάνοντας έτσι ή και ξεπερνώντας τα αντίστοιχα ποσοστά διείσδυσης στον πληθυσμό της παραδοσιακής σταθερής τηλεφωνίας.

Οι υπηρεσίες κινητών επικοινωνιών 2G παρέχουν στον κάθε χρήστη αμφίδρομη φωνητική επικοινωνία ισοδύναμου εύρους ζώνης ψηφιακών δεδομένων περίπου 4-40 Kbps (1 Kbps = ρυθμός μετάδοσης 1.024 δυαδικών ψηφίων, 0 ή 1, ανά δευτερόλεπτο).

Λίγο πριν από τη μετάβαση στην επόμενη γενιά (3G), οι κινητές επικοινωνίες πέρασαν από το στάδιο της μετάδοσης ψηφιακών δεδομένων σε σχετικά υψηλότερες ταχύτητες, π.χ. με τις υπηρεσίες GPRS (General Packet Radio Service), EDGE (Enhanced Data for GSM Evolution) και HSCSD (High Speed Circuit Switched Data). Η γενιά αυτή έμεινε γνωστή σαν 2G5 ή 2.5G, δηλ. «ενδιάμεση γενιά μεταξύ 2G και 3G» και προβλέπει εύρος ζώνης ανά χρήστη από 56 Kbps έως 384 Kbps.

Σήμερα βρίσκεται σε πλήρη ανάπτυξη η 3η γενιά κινητών επικοινωνιών, γνωστή με τα ονόματα UMTS (Universal Mobile Telecommunication System, ευρωπαϊκό standard βασισμένο στις τεχνολογίες Wideband CDMA και Time-Division CDMA) και CDMA2000.

Οι υπηρεσίες κινητών επικοινωνιών 3ης Γενιάς (3Γ ή 3G) προβλέπουν εύρος ζώνης ανά χρήστη από 384 Kbps έως 2048 Kbps και διάδοση ενοποιημένης πολυμεσικής πληροφορίας (ήχου, εικόνας, video και δεδομένων). Πρωτοπόρος στη ευρεία εφαρμογή αυτών των υπηρεσιών είναι η Ιαπωνία (με το γνωστό «iMode» από την εταιρεία NTT DoCoMo, που ξεκίνησε από το 1999, με 26 εκ. συνδρομητές τα πρώτα 2,5 χρόνια και αρχικό ρυθμό

διείσδυσης 50 χιλ. χρήστες ανά ημέρα). Λόγω του iMode, το 2001, 80% των κινητών χρηστών του Internet βρίσκονταν στην Ιαπωνία, 12,5% στην Κορέα, 5% στην Ευρώπη και 1% στην Αμερική. Σήμερα, τα ποσοστά αυτά έχουν αλλάξει δραστικά και οι αριθμοί μεταβάλλονται ραγδαία σε καθημερινή βάση [1].

Μέσα στο 2005, άρχισε να διατίθεται σε εμπορική χρήση στις ΗΠΑ, Γερμανία, Γαλλία, Αγγλία, Φινλανδία, Σουηδία κ.λπ. η υπηρεσία «κινητής τηλεόρασης» (mobile TV), βασισμένη στην τεχνολογία DVB-H (Digital Video Broadcasting – Handheld, υπηρεσία πολυεκπομπής ψηφιακού video).

Λόγω του ότι οι επενδύσεις των παρόχων κινητών επικοινωνιών σε υποδομές 3G ήταν και είναι σημαντικές (τόσο σε φάσμα συχνοτήτων, όσο και σε εξοπλισμό), αναμένεται ότι η γενιά 3G θα παραμείνει σε φάση ωρίμασης για περίπου 3-5 χρόνια ακόμη. Αυτό σημαίνει ότι σήμερα οι τεχνολογίες της επόμενης γενιάς κινητών επικοινωνιών («μετά την 3η Γενιά» Beyond-3G ή B3G ή κατ' άλλους 4Γ ή 4G) ήδη αναπτύσσονται σε πειραματικό επίπεδο, σε κορυφαία ερευνητικά κέντρα παγκοσμίως.

Ποια είναι όμως τα χαρακτηριστικά των συστημάτων και υπηρεσιών B3G; Πρόκειται για τις νέες τεχνολογίες κινητής επικοινωνίας, που αναμένονται εμπορικά γύρω στο 2010 και θα παρέχουν τη δυνατότητα ασφαλών και αξιόπιστων οικουμενικών (ubiquitous, δηλ. παντού και πάντα διαθέσιμων) υπηρεσιών σε χρήστες περιορισμένης ή και μεγάλης κινητικότητας. Οι τεχνολογίες αυτές έχουν δύο βασικές συνιστώσες: τις «ραδιο-τεχνολογίες B3G» (ή τεχνολογίες μετάδοσης σήματος) και τις «υπηρεσίες B3G», δηλ. τις εφαρμογές που παρέχονται στον τελικό χρήστη.

Οι «Ραδιο-τεχνολογίες B3G» αναμένεται να έχουν τα εξής χαρακτηριστικά:

- Υψηλότερους ρυθμούς μετάδοσης από την 3G, με κορύφωση (peak) τα 20-200 Mbps.
- Καλύτερη αξιοποίηση του διαθέσιμου φάσματος και μικρότερο κόστος ανά bit.
- Προσαρμογή φυσικής και λογικής πρόσβασης (physical & MAC interface) που ελέγχεται από λογισμικό (software controlled radios) και βελτιστοποιείται για IP κυκλοφορία, με χρήση του πρωτοκόλλου IPv6 (all IPv6 δίκτυα μεταφοράς) και εγγυήσεις ποιότητας υπηρεσιών (QoS), που σχετίζονται με βέλτιστη χρήση του φάσματος και της μπαταρίας, ανάλογα με τα δεδομένα του δικτύου και τις απαιτήσεις του χρήστη.

- Μικρότερες κυψέλες (cells), για την επίτευξη των ζητούμενων μεγαλύτερων ρυθμών μετάδοσης, για τον ίδιο πληθυσμό.
- Υψηλότερες χρησιμοποιούμενες συχνότητες (μέχρι 5 GHz), με εύρος ζώνης ραδιοσυχνοτήτων (RF) ανά κανάλι 20~100 MHz.
- Χρησιμοποίηση πολλαπλών κεραιών, τόσο στους σταθμούς βάσης όσο και στις κινητές συσκευές, με χρήση του πρωτοκόλλου ορθογώνιας πολυπλεξίας συχνότητας, OFDM (Orthogonal Frequency Division Multiplexing), αλλά και άλλων μεθόδων.
- Εναρμονισμός του χρησιμοποιούμενου φάσματος σε παγκόσμια βάση.

Οι «Υπηρεσίες B3G» σχεδιάζονται με τα εξής επιθυμητά χαρακτηριστικά:

- Υποστήριξη ευρυζωνικότητας και πολυμεσικότητας (broadband, multimedia services).
- Υψηλή ασφάλεια (security) και ανοχή σε σφάλματα (fault-tolerance) στις επικοινωνίες, προσαρμοζόμενη δυναμικά στις απαιτήσεις του κάθε δικτύου και του εκάστοτε χρήστη και σε συνδυασμό με τη βέλτιστη χρήση των πόρων (φάσμα, μπαταρία, QoS) της κινητής συσκευής.
- Συγκεκριμένα, εξατομικευμένα χαρακτηριστικά ασφάλειας και πιστοποιητικά ασφάλειας (security certificates) για κάθε παρεχόμενη υπηρεσία B3G και για κάθε κινητή συσκευή. Οποιαδήποτε πρόσβαση θα γίνεται μόνο εφόσον τα πιστοποιητικά πρόσβασης και των δύο πλευρών είναι αμοιβαία αποδεκτά (από τον πάροχο της υπηρεσίας και από τον χρήστη).
- Διασυνδεσιμότητα παντού, με πλήθος δικτύων (σταθερά, κινητά, ad-hoc) και διαφόρων παρόχων (ubiquitous connectivity), με τρόπο διαφανή για το χρήστη. Δηλ. καθώς ο χρήστης μετακινείται, ενώ π.χ. είναι συνδεδεμένος με το Internet ή συμμετέχει σε video-τηλεδιάσκεψη, θα μπορεί να αλλάζει δίκτυα (UMTS, WiFi, Bluetooth, κ.λπ.) και παρόχους, με τρόπο αυτόματο, χωρίς να διακόπτεται η σύνδεσή του (seamless handoffs) και ισορροπώντας βέλτιστα μεταξύ ασφάλειας, ποιότητας σύνδεσης (QoS) και κόστους της παρεχόμενης υπηρεσίας.
- Αυτόματη, έξυπνη και δυναμική διαπραγμάτευση όρων, κριτηρίων και συνθηκών πρόσβασης σε διάφορες υπηρεσίες και δίκτυα (service level agreements, SLA).

- Ανοιχτές αρχιτεκτονικές ανάπτυξης λογισμικού με επιθυμητή την παγκόσμια σύγκλιση σε κοινά standards (πρωτόκολλα και πλατφόρμες ανάπτυξης).

Ενδεικτικά αναφέρουμε ορισμένες τέτοιες μελλοντικές υπηρεσίες B3G:

- Συμμετοχή σε e-ψηφοφορίες και e-εκλογές με το κινητό τηλέφωνο (με ασφάλεια, αξιοπιστία και εμπιστευτικότητα).
- Συμμετοχή σε e-δημοσκοπήσεις και e-αξιολογήσεις (με τρόπο διακριτικό και επιλεκτικό).
- Ιατρική τηλε-παρακολούθηση ασθενών και ηλικιωμένων (με έμφαση στην εμπιστευτικότητα και αξιόπιστη μετάδοση των προσωπικών δεδομένων).
- Ανοικτή και εξ αποστάσεως τηλε-εκπαίδευση και τηλε-κατάρτιση (με διαχείριση πολυμεσικού υλικού από κινούμενους χρήστες (σπουδαστές, συμβούλους καθηγητές, δημιουργούς) και συνδρομητικό και ASP (Application Service Provider) μοντέλο παροχής των υπηρεσιών.
- Τηλε-εργασία και online τηλε-βοήθεια στην εργασία, με χρήση φορητών πολυμεσικών συσκευών.
- Δικτυακά, πολυμεσικά, ευρυζωνικά τηλε-παιχνίδια με παγκόσμια κατανεμημένους κινούμενους χρήστες.
- Διαδραστική, επιλεκτική, κινητή τηλεόραση και video, όπου, το καθημερινό πρόγραμμα που θα παρακολουθεί ο χρήστης θα διαμορφώνεται ανάλογα με το προφίλ του και τις επιθυμίες του, σε πραγματικό χρόνο.

Παράλληλα, η εξέλιξη και η επιτυχής επέκταση των τοπικών ασύρματων δικτύων (WLAN) παγκοσμίως έχουν παραγάγει την απαίτηση για ενσωμάτωση με τα κινητά δίκτυα τρίτης γενιάς (3G). Ο βασικός στόχος αυτής της ενσωμάτωσης είναι να αναπτυχθούν ετερογενή κινητά δίκτυα δεδομένων, ικανά να υποστηρίζουν τις νέες αναδυόμενες υπηρεσίες δεδομένων οι οποίες απαιτούν υψηλούς ρυθμούς μεταφοράς. Η προσπάθεια να αναπτυχθούν τέτοια ετερογενή δίκτυα, B3G, υλοποιεί το όραμα για τα ασύρματα συστήματα επόμενης γενιάς, τα οποία υπόσχονται να παρέχουν καθολική υπολογιστική παρουσία (ubiquitous computing) στους τελικούς χρήστες.

Η δικτυακή αρχιτεκτονική που ενσωματώνει το 3G και το WLAN ορίζει δύο διαφορετικά σενάρια πρόσβασης: (α) την άμεση IP πρόσβαση WLAN και (β) την πρόσβαση WLAN 3GPP IP. Το πρώτο σενάριο παρέχει στον χρήστη σύνδεση IP στο Διαδίκτυο ή σε ένα ενδοδίκτυο (intranet) μέσω ενός δικτύου πρόσβασης WLAN (WLAN-AN), ενώ το δεύτερο

επιτρέπει στον χρήστη να συνδεθεί σε υπηρεσίες 3G Packet Switch, όπως είναι το Wireless Application Protocol (WAP) και το Mobile Multimedia Services (MMS), ή στο Διαδίκτυο μέσω του 3G Public Land Mobile Network (PLMN). Το νέο αυτό μοντέλο δικτύωσης, δηλαδή του 3G μαζί με του WLAN, θέτει νέες προκλήσεις κυρίως όσον αφορά την ασφάλεια λόγω της πολυπλοκότητας της αρχιτεκτονικής και της ετερογένειας των τεχνολογιών που χρησιμοποιούνται. Κατά συνέπεια ο σωστός σχεδιασμός και η αναλυτική αξιολόγηση των μηχανισμών ασφάλειας που χρησιμοποιούνται στην αρχιτεκτονική δικτύωσης 3G-WLAN είναι ζωτικής σημασίας για την αποτελεσματική ενσωμάτωση των διαφορετικών τεχνολογιών κατά τρόπο ασφαλή.

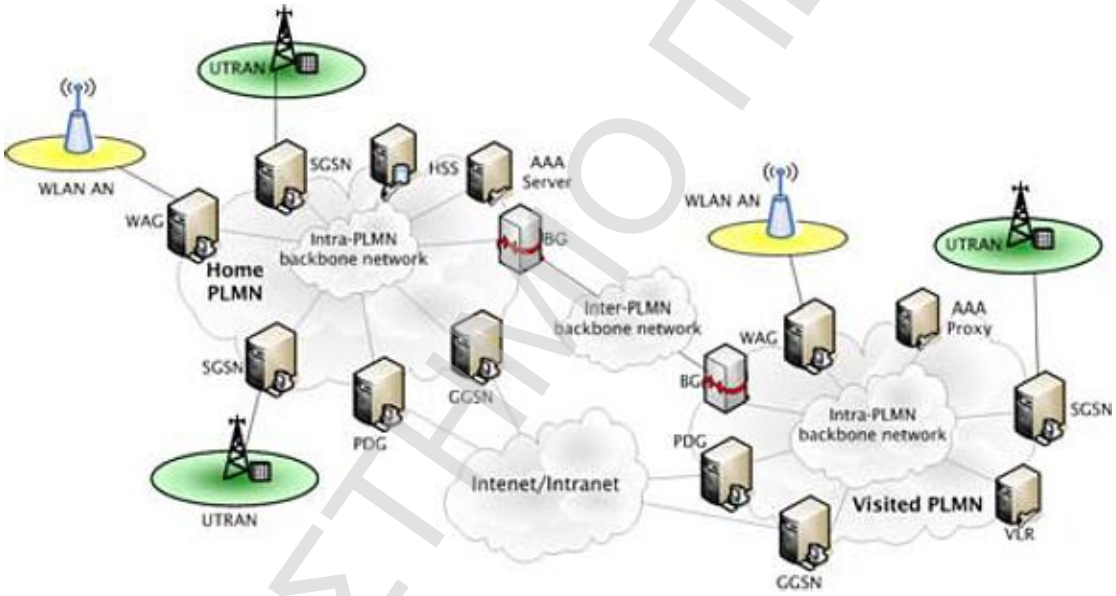
4.2 Αρχιτεκτονική ενός δικτύου B3G

Όπως φαίνεται στην Εικόνα 6, η αρχιτεκτονική ενός δικτύου B3G αποτελείται από τρία ανεξάρτητα τμήματα:

1. το WLAN Access Network (WLAN-AN),
2. το 3G VPLMN (Visited PLMN). Το Visited PLMN είναι το PLMN στο οποίο περιφέρεται ο χρήστης.
3. το κεντρικό 3G HPLMN (Home PLMN). Το κεντρικό PLMN υποδηλώνει το PLMN στο οποίο ανήκει ο χρήστης.

Η Εικόνα 6 απεικονίζει την αρχιτεκτονική δικτύωσης του 3GPP με το WLAN. Το WLAN-AN είναι ένα δίκτυο πρόσβασης WLAN που έχει περισσότερα από ένα WLAN Access Points (AP). Τα ασύρματα σημεία πρόσβασης ενεργούν ως clients που παρέχουν πιστοποίηση, εξουσιοδότηση και διαχείριση λογαριασμών (Authentication, Authorization, Accounting ή AAA) [10]. Ο 3GPP AAA Proxy εκτελεί λειτουργίες φιλτραρίσματος και διαμεσολάβησης στο visited δίκτυο. Ο διακομιστής AAA ανακτά τις πληροφορίες πιστοποίησης και το προφίλ των συνδρομητών από τον διακομιστή HSS (Home Subscriber Server) στο 3GPP home δίκτυο συνδρομητών. Ο HSS παρέχει λειτουργίες κέντρου πιστοποίησης AuC (Authentication Centre) και HLR (Home Location Register). Το WAG (WLAN Access Gateway) είναι μια πύλη για τα δεδομένα από και προς το WLAN-AN και το UE (User Equipment). Οι υπηρεσίες PS 3GPP

μπορούν να χρησιμοποιηθούν μέσω ενός PDG (Packet Data Gateway) στο home δίκτυο του χρήστη ή στο επιλεγμένο visited δίκτυο. Το SGSN (Serving GPRS Support Node) είναι μια πύλη για την πρόσβαση του κεντρικού δικτύου πακέτων (core network). Το GGSN (Gateway GPRS Support Node) είναι μια πύλη για την πρόσβαση των υπηρεσιών 3GPP PS ή ενός εξωτερικού δίκτυου που βασίζεται στο IP, και τέλος το PDG έχει την ίδια λειτουργία με το GGSN. Το WLAN UE είναι ένα κινητό τερματικό με USIM (User Subscriber Identity Module) το οποίο περιέχει την μονάδα UMTS και την μονάδα WLAN με τα πρωτόκολλα σηματοδότησης και δεδομένων για κάθε σύστημα.



Εικόνα 6. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΚΤΥΟΥ B3G

Η αρχιτεκτονική των δικτύων B3G ορίζει δύο διαφορετικά σενάρια πρόσβασης στο δίκτυο [4]: (α) άμεση IP πρόσβαση WLAN και (β) πρόσβαση WLAN 3GPP IP. Το πρώτο σενάριο παρέχει σε έναν χρήστη σύνδεση στο Διαδίκτυο ή σε ένα ενδοδίκτυο μέσω του WLAN-AN. Σε αυτό το σενάριο και ο χρήστης και το δίκτυο επικυρώνονται ο ένας στον άλλο χρησιμοποιώντας το πρωτόκολλο EAP-SIM [15] ή το EAP-AKA [19]. Το σενάριο πρόσβασης WLAN 3GPP IP επιτρέπει σε έναν χρήστη να συνδεθεί με τις υπηρεσίες PS (όπως WAP, MMS, LBS, κ.λπ.) ή με το Διαδίκτυο μέσω του 3G PLMN. Σε αυτό το σενάριο, ο χρήστης επικυρώνεται στο 3G PLMN χρησιμοποιώντας το EAP-SIM ή το πρωτόκολλο EAP-AKA που ενθυλακώνεται μέσα σε μηνύματα IKEv2 [11].

4.3 Αρχιτεκτονικές ασφάλειας για δίκτυα B3G

Κάθε σενάριο πρόσβασης (δηλ., άμεση πρόσβαση WLAN και πρόσβαση WLAN 3GPP IP) στα δίκτυα B3G, ενσωματώνει μια συγκεκριμένη αρχιτεκτονική ασφάλειας η οποία στοχεύει στην προστασία των συμβαλλόμενων μερών (δηλ. τους κινητούς χρήστες, το WLAN και το 3G δίκτυο) και των δεδομένων που ανταλλάσσονται μεταξύ τους. Αυτές οι αρχιτεκτονικές [2] αποτελούνται από διάφορα πρωτόκολλα ασφάλειας που παρέχουν αμοιβαία πιστοποίηση. Στην συνέχεια, παρουσιάζονται και αναλύονται οι αρχιτεκτονικές ασφάλειας και τα πρωτόκολλα ασφάλειας που υιοθετούνται στα δίκτυα B3G.

4.3.1 EAP

Το επεκτάσιμο πρωτόκολλο πιστοποίησης (Extensible Authentication Protocol) ή EAP, είναι ένα καθολικό πλαίσιο πιστοποίησης που χρησιμοποιείται συχνά στα ασύρματα δίκτυα και από τις Σημείο-σε-Σημείο συνδέσεις. Το EAP περιγράφεται στο RFC 3748 [7]. Αν και το πρωτόκολλο EAP δεν περιορίζεται μόνο σε ασύρματα LAN και μπορεί να χρησιμοποιηθεί για πιστοποίηση σε ενσύρματο LAN, χρησιμοποιείται συχνότερα σε ασύρματο LAN. Πρέπει να τονιστεί ότι το EAP είναι ένα πλαίσιο πιστοποίησης και όχι ένας συγκεκριμένος μηχανισμός πιστοποίησης. Το EAP παρέχει μερικές κοινές λειτουργίες και παρέχει διαπραγμάτευση του επιθυμητού μηχανισμού πιστοποίησης. Τέτοιοι μηχανισμοί καλούνται μέθοδοι EAP και σήμερα υπάρχουν περίπου 40 διαφορετικές μέθοδοι. Οι μέθοδοι που καθορίζονται σε διάφορα IETF RFC περιλαμβάνουν τις EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EAP-AKA και άλλες λιγότερο χρησιμοποιούμενες. Οι πιο ευρέως χρησιμοποιημένες σύγχρονες μέθοδοι που είναι ικανές να λειτουργούν σε ασύρματα δίκτυα περιλαμβάνουν τις EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP και EAP-TTLS. Οι προδιαγραφές για τις μεθόδους EAP που χρησιμοποιούνται για την πιστοποίηση σε LAN περιγράφονται στο RFC 4017 [12].

Όταν το EAP καλείται από μία συσκευή NAS (Network Access Server) που υποστηρίζει το 802.1X, π.χ ένα ασύρματο σημείο πρόσβασης 802.11 a/b/g, οι σύγχρονες μέθοδοι EAP μπορούν να παρέχουν έναν ασφαλή μηχανισμό πιστοποίησης και να διαπραγματευτούν ένα ασφαλές PMK (Pair-wise Master Key) μεταξύ του client και του NAS. Το PMK μπορεί έπειτα να χρησιμοποιηθεί για την ασύρματη σύνοδο κρυπτογράφησης που χρησιμοποιεί την

κρυπτογράφηση TKIP ή CCMP (βασισμένη σε AES). Το EAP δεν είναι ένα πρωτόκολλο καλωδίου, αντ' αυτού καθορίζει μόνο την μορφή των μηνυμάτων. Κάθε πρωτόκολλο που χρησιμοποιεί το EAP καθορίζει έναν τρόπο για να ενθυλακωθούν τα μηνύματα EAP μέσα στα μηνύματα του πρωτοκόλλου. Στην περίπτωση του 802.1X, αυτή η ενθυλάκωση καλείται EAPOL, «EAP over LANs».

4.3.2 Περίπτωση πρόσβασης WLAN Direct IP

Στην περίπτωση άμεσης πρόσβασης IP στο WLAN, και ο χρήστης αλλά και το δίκτυο πιστοποιούνται ο ένας στον άλλο χρησιμοποιώντας το EAP-SIM ή το EAP-AKA, τα οποία είναι βασισμένα στο πρωτόκολλο 802.1X [18]. Εφόσον η πιστοποίηση γίνει επιτυχώς, ο χρήστης λαμβάνει μια διεύθυνση IP από το WLAN-AN και έπειτα αποκτά πρόσβαση στο Διαδίκτυο ή σε ένα ενδοδίκτυο, ανάλογα με την απαιτούμενη υπηρεσία. Σε αυτήν την περίπτωση, η εμπιστευτικότητα και η ακεραιότητα των δεδομένων του χρήστη που μεταβιβάζονται από το WLAN εξασφαλίζονται από τους μηχανισμούς ασφάλειας του πρωτοκόλλου 802.11i [17], που θα αναλυθούν παρακάτω.

Το συγκεκριμένο πρωτόκολλο ασφάλειας (EAP-AKA ή EAP-SIM) που θα χρησιμοποιηθεί για την αμοιβαία πιστοποίηση μεταξύ του χρήστη και του δικτύου, εξαρτάται από τη συνδρομή του χρήστη. Εάν ο χρήστης κατέχει μια κάρτα UMTS Subscribers Identity Module (USIM) [5] τότε χρησιμοποιείται το πρωτόκολλο EAP-AKA. Διαφορετικά, χρησιμοποιείται το πρωτόκολλο EAP-SIM σε περιπτώσεις που ο χρήστης έχει μια κάρτα SIM [14] GSM ή GPRS. Όταν ο διακομιστής AAA λαμβάνει την ταυτότητα του χρήστη, προσκομίζει από το HSS/HLR το προφίλ του χρήστη προκειμένου να καθοριστεί το πρωτόκολλο πιστοποίησης που θα χρησιμοποιηθεί. Παρακάτω, αναλύουμε τη λειτουργία αυτών των δύο πρωτοκόλλων και εστιάζουμε στις υπηρεσίες ασφάλειας που παρέχει το καθένα.

Πρότυπο 802.11i

Το πρότυπο 802.11i χρησιμοποιείται για την παροχή υπηρεσιών εμπιστευτικότητας και ακεραιότητας στα δεδομένα που διαβιβάζονται ασύρματα στην περίπτωση της πρόσβασης WLAN Direct IP. Το 802.11i δημιουργήθηκε για να ενισχύσει τις υπηρεσίες ασφάλειας των

WLAN. Η σχεδίαση του βασίστηκε στο γεγονός ότι το πρωτόκολλο WEP δεν μπορούσε να καλύψει πλήρως τις απαιτήσεις ασφαλείας των WLAN [20]. Έτσι ο ρόλος του προτύπου 802.11i είναι διπλός:

1. να παρέχει διαχείριση των κλειδιών συνόδου ορίζοντας την τετραπλή χειραψία (four way handshake) και διαδικασίες χειραψίας κλειδιού ομάδας (group key handshake)

2. να ενισχύσει την παροχή υπηρεσιών ασφαλείας στα δεδομένα του χρήστη ενσωματώνοντας δύο πρωτόκολλα ασφαλείας: (α) το Counter-Mode/CBC-MAC Protocol (CCMP) το οποίο χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης AES και (β) το Temporal Key Integrity Protocol (TKIP) το οποίο χρησιμοποιεί την ίδια μέθοδο κρυπτογράφησης με το WEP.

EAP-SIM

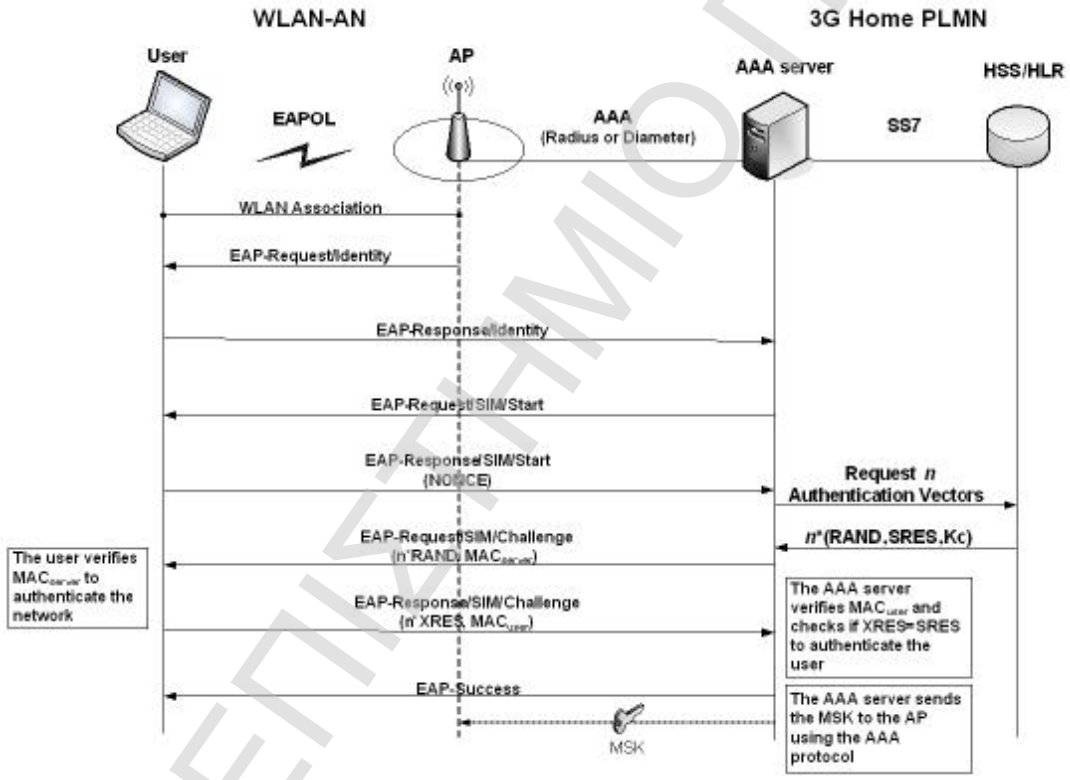
Το EAP-SIM [11] παρέχει αμοιβαία πιστοποίηση σε δικτυακό περιβάλλον που ενσωματώνει 3G και WLANs, χρησιμοποιώντας τα πιστοποιητικά που περιλαμβάνονται σε μια κάρτα SIM μιας συνδρομής GSM/GPRS. Περιλαμβάνει έναν χρήστη, έναν AAA client (που είναι συνήθως ασύρματο σημείο πρόσβασης) και έναν διακομιστή AAA που λαμβάνει τις πληροφορίες πιστοποίησης από το HSS/HLR του δικτύου όπου ο χρήστης είναι συνδρομητής. Το πρωτόκολλο EAP-SIM ενσωματώνει δύο βασικές βελτιώσεις που εξαλείφουν γνωστές αδυναμίες ασφάλειας της πιστοποίησης και της διαδικασίας συμφωνίας κλειδιού (key agreement) σε GSM/GPRS [11]. Κατ' αρχάς, το κλειδί που χρησιμοποιείται για την κρυπτογράφηση ενισχύεται έτσι ώστε να έχει 128 bits σε αντίθεση με την εξηντατετράμπιτη ασφάλεια του αρχικού κλειδιού GSM/GPRS. Δεύτερον, το EAP-SIM υποστηρίζει την αμοιβαία πιστοποίηση, σε αντίθεση με την πιστοποίηση GSM/GPRS, η οποία εκτελεί μόνο πιστοποίηση του χρήστη στο δίκτυο (user-to-network).

Για την δημιουργία πιο ισχυρών κλειδιών, το πρωτόκολλο EAP-SIM συνδυάζει *n* (με *n*=2 ή *n*=3) ανεξάρτητα RAND που έχουν σαν αποτέλεσμα την παραγωγή *n* κλειδιών συνόδου (session keys), Kc. Αυτά τα κλειδιά συνδυάζονται με έναν τυχαίο αριθμό (NONCE), με την ταυτότητα του χρήστη *Identity* και άλλες συναφείς με το περιεχόμενο πληροφορίες για την δημιουργία του κύριου κλειδιού *MK* (Master Key) του πρωτοκόλλου EAP-SIM βάσει του τύπου

$$MK = SHA1(Identity + n*Kc + NONCE + Version\ List + Selected\ Version) \quad (1)$$

όπου SHA1 είναι μια συνάρτηση κατακερματισμού [13]. Στη συνέχεια, το κλειδί *MK* χρησιμοποιείται σαν είσοδος σε μια ψευδό τυχαία συνάρτηση F που παράγει τα υπόλοιπα κλειδιά που χρησιμοποιούνται στο EAP-SIM. Από αυτά τα κλειδιά τα πιο σημαντικά είναι

- το κύριο κλειδί της συνόδου *MSK* (Master Session Key), που χρησιμοποιείται στο πρωτόκολλο 802.11i για την δημιουργία των κλειδιών κρυπτογράφησης
- και το κλειδί *K_auth* που χρησιμοποιείται στο EAP-SIM για τη δημιουργία συντονισμένων κωδικών πιστοποίησης μηνύματος (Message Authentication Codes, MACs) για σκοπούς πιστοποίησης.



Εικόνα 7. Διαδικασία πιστοποίησης EAP-SIM

Η Εικόνα 7 απεικονίζει την ανταλλαγή μηνυμάτων στο EAP-SIM ανάμεσα στον χρήστη και στον διακομιστή AAA. Ο χρήστης επικοινωνεί με το ασύρματο σημείο πρόσβασης μέσω του πρωτοκόλλου EAPOL [7]. Αρχικά ο χρήστης επικοινωνεί με το ασύρματο σημείο πρόσβασης, το οποίο στέλνει ένα μήνυμα EAP-Request/Identity στον χρήστη ρωτώντας τον για την ταυτότητά του. Ο χρήστης απαντά με ένα μήνυμα EAP- Response/Identity το οποίο

περιλαμβάνει την ταυτότητά του σε μορφή NAI (Network Access Identifier) [6]. Η ταυτότητα του χρήστη μπορεί να είναι είτε σε μορφή IMSI (International Mobile Subscriber Identity), ή μία προσωρινού τύπου ταυτότητα (π.χ ένα ψευδώνυμο). Γνωρίζοντας την ταυτότητα του χρήστη ο διακομιστής AAA αποστέλλει ένα μήνυμα EAP-Request/SIM/Start με αποτέλεσμα να εκκινεί την διαδικασία πιστοποίησης. Ο χρήστης απαντά με ένα μήνυμα EAP-Response/SIM/Start που περιέχει μια παράμετρο NONCE, που είναι η εξακρίβωση του χρήστη στο δίκτυο. Με την λήψη αυτού του μηνύματος ο διακομιστής AAA επικοινωνεί με το HSS/HLR και αποκτά *n* (*n*=2 ή *n*=3) τριπλέτες πιστοποίησης (RAND, SRES, Kc) για τον συγκεκριμένο χρήστη, ο οποίος είναι ο ιδιοκτήτης την κάρτας SIM. Η δημιουργία των τριπλετών πιστοποίησης GSM βασίζεται σε ένα μόνιμο μυστικό κλειδί ***Ki,*** το οποίο γνωρίζουν ο χρήστης και το δίκτυο, και που ανατίθεται στον χρήστη όταν συνδέεται στο δίκτυο GSM/GPRS. Στη συνέχεια ο διακομιστής AAA στέλνει στον χρήστη ένα μήνυμα EAP-Request/SIM/Challenge το οποίο περιέχει *n* RANDs και το MAC διακομιστή του μηνύματος που υπολογίζεται χρησιμοποιώντας το κλειδί *K_auth ως εξής:*

$$MAC_{διακομιστή} = HMAC\_SHA1_{K\_auth}(EAP\text{-}Request/SIM/Challenge(n*RAND) + NONCE) \quad (2)$$

όπου το HMAC-SHA1 [16] είναι ο αλγόριθμος MAC που παράγει την τιμή κατακερματισμού. Πριν τον υπολογισμό της τιμής $MAC_{διακομιστή}$ ο διακομιστής AAA πρέπει πρώτα να παραγάγει το κλειδί *MK και στη συνέχεια τα κλειδιά* ***K_auth*** και ***MSK***. Μετά την λήψη του μηνύματος EAP-Request/SIM/Challenge, η πλευρά του χρήστη εκτελεί τους αλγόριθμους πιστοποίησης GSM/GPRS *n φορές,* μία για κάθε RAND που λαμβάνει, έτσι ώστε να παραγάγει τα *n* Kc κλειδιά και τις *n τιμές* XRES. Στη συνέχεια παράγεται το κλειδί *MK και τα* κλειδιά ***K_auth*** *και* ***MSK***. Στη συνέχεια ο χρήστης επαληθεύει το $MAC_{διακομιστή}$ χρησιμοποιώντας το κλειδί ***K_auth*** και εάν αυτός ο έλεγχος είναι επιτυχής τότε το δίκτυο πιστοποιείται στον χρήστη και ο χρήστης διαβιβάζει στον διακομιστή AAA τις παραγόμενες *n* XRES τιμές με ένα μήνυμα EAP-Response/SIM/Challenge. Αυτό το μήνυμα περιέχει την τιμή $MAC_{χρήστη}$ που παράγεται ως εξής:

$$MAC_{χρήστη} = HMAC\text{-}SHA1_{K\_auth}(EAP\text{-}Response/SIM/Challenge(n*XRES) + n*XRES) \quad (3)$$

Με το που λάβει το μήνυμα ο διακομιστής AAA ελέγχει εάν το $MAC_{χρήστη}$ είναι έγκυρο και εάν οι *n* τιμές XRES είναι ίσες με τις *n τιμές* SRES που έχει λάβει από το HSS/HLR για την πιστοποίηση. Εάν ο έλεγχος επιτύχει τότε ο διακομιστής AAA στέλνει ένα μήνυμα EAP-Success στον χρήστη δηλώνοντας έτσι την επιτυχή πιστοποίηση και επιπρόσθετα στέλνει στο

ασύρματο σημείο πρόσβασης το κλειδί συνόδου *MSK*. Σε αυτό το σημείο και ο χρήστης αλλά και το δίκτυο έχουν πιστοποιηθεί αμοιβαία, και επίσης το ασύρματο AP μοιράζεται με τον χρήστη το κλειδί *MSK*, που χρησιμοποιείται στο πρωτόκολλο 802.11i.

EAP-AKA

Το EAP-AKA [19] (Authentication and Key Agreement, AKA) αποτελεί ένα εναλλακτικό πρωτόκολλο πιστοποίησης του EAP-SIM και χρησιμοποιεί μια κάρτα USIM και την διαδικασία πιστοποίησης και συμφωνίας κλειδιού UMTS. Περιλαμβάνει τα ίδια στοιχεία δικτύου με το EAP-SIM (τον χρήστη, τον πελάτη AAA και τον διακομιστή AAA). Όπως και στο EAP-SIM, στα πρώτα δύο μηνύματα της διαπραγμάτευσης στο EAP-AKA το ασύρματο AP ζητά την ταυτότητα του χρήστη ο οποίος απαντά στέλνοντας ένα μήνυμα EAP response/identity που περιέχει την μόνιμη ή την προσωρινή ταυτότητα του μέσα σε μορφή NAI. Μετά την λήψη της ταυτότητας χρήστη, ο διακομιστής AAA ελέγχει εάν κατέχει ένα 3G διάνυσμα πιστοποίησης που έχει αποθηκευτεί από μια προηγούμενη πιστοποίηση με τον συγκεκριμένο χρήστη. Εάν κάτι τέτοιο δεν ισχύει, ο διακομιστής AAA στέλνει την ταυτότητα IMSI χρήστη στο HSS/HLR. Το HSS/HLR παραγάγει *n* διανύσματα πιστοποίησης για τον συγκεκριμένο χρήστη χρησιμοποιώντας το μόνιμο μυστικό κλειδί K του UMTS, που έχει ανατεθεί στον χρήστη όταν έχει εγγραφεί στο δίκτυο και το στέλνει στον διακομιστή AAA. Ένα διάνυσμα πιστοποίησης εμπεριέχει ένα RAND, το σύμβολο πιστοποίησης AUTN, την αναμενόμενη απάντηση XRES, το κλειδί κρυπτογράφησης *CK* και το κλειδί ακεραιότητας *IK* [8]. Στη συνέχεια ο διακομιστής AAA επιλέγει ένα από τα *n* διανύσματα πιστοποίησης για να προχωρήσει με την διαδικασία πιστοποίησης EAP-AKA και αποθηκεύει τα υπόλοιπα *n*-1 για μελλοντική χρήση. Ο υπολογισμός του κύριου κλειδιού *MK του* EAP-AKA γίνεται ως εξής:

$$MK = SHA1(Identity + IK + CK) \quad (4)$$

Το *MK* χρησιμοποιείται για την δημιουργία του MSK και του κλειδιού *K_auth*. Ο διακομιστής AAA χρησιμοποιεί το κλειδί *K_auth* για τον υπολογισμό του $MAC_{διακομιστή}$ όπου επαληθεύει την ακεραιότητα του επόμενου μηνύματος EAP-AKA (EAP-Request/AKA-Challenge).

$$MAC_{διακομιστή} = HMAC\text{-}SHA1_{K\_auth}(EAP\text{-}Request/AKA/Challenge(RAND,AUTN)) \quad (5)$$

Ο διακομιστής AAA στέλνει το μήνυμα EAP-Request/AKA-Challenge στον χρήστη ο οποίος εκτελεί τους αλγορίθμους UMTS-AKA και επαληθεύει το AUTN [8]. Στη συνέχεια παραγάγει τα κλειδιά *IK* και *CK* για τον υπολογισμό του κλειδιού *MK*. Έπειτα χρησιμοποιεί το κλειδί *MK* για τον υπολογισμό του κλειδιού *MSK και του K_auth*, για την επαλήθευση της τιμής $MAC_{διακομιστή}$. Εάν αυτές οι επαληθεύσεις γίνουν με επιτυχία, ο χρήστης υπολογίζει την τιμή XRES και στέλνει ένα μήνυμα EAP-Response/AKA-challenge στον διακομιστή AAA και υπολογίζεται χρησιμοποιώντας το κλειδί *K_auth:*

$$MAC_{χρήστη}=HMAC\text{-}SHA1_{K\_auth}(EAP\text{-}Response/AKA/Challenge(n*XRES)) \quad (6)$$

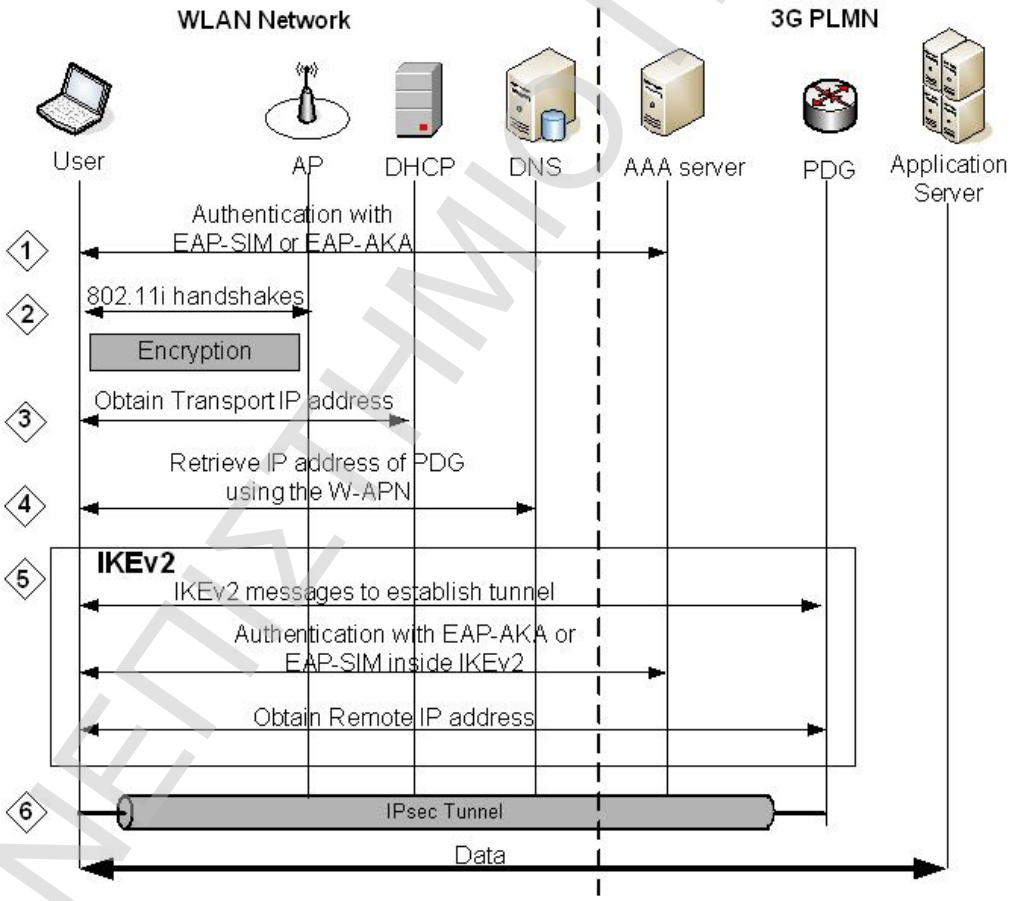
Αφού ο διακομιστής AAA λάβει το μήνυμα EAP-Response/AKA-challenge, επαληθεύει την τιμή $MAC_{χρήστη}$ που έχει λάβει και ελέγχει εάν η απάντηση του χρήστη XRES ταιριάζει με την απάντηση SRES από το HLR/HSS. Εάν όλοι αυτοί οι έλεγχοι γίνουν επιτυχώς, ο διακομιστής AAA αποστέλλει ένα μήνυμα EAP-success μαζί με το κλειδί *MSK* στο ασύρματο AP. Το AP αποθηκεύει το κλειδί και το προωθεί στον χρήστη. Φτάνοντας στο τελικό στάδιο του πρωτοκόλλου EAP-AKA, υπάρχει αμοιβαία πιστοποίηση του χρήστη και του δικτύου και ο χρήστης μοιράζεται το κλειδί *MSK* με το ασύρματο *AP*. Το κλειδί αυτό χρησιμοποιείται στο πρότυπο 802.11i για την δημιουργία των κλειδιών κρυπτογράφησης συνόδου.

Επίσης, στο EAP-AKA υπάρχουν δύο διαδικασίες πιστοποίησης: Η πλήρης πιστοποίηση και η γρήγορη επαναπιστοποίηση. Η πλήρης πιστοποίηση είναι μια αρχική διαδικασία επικύρωσης όπου τα νέα κλειδιά παράγονται στην κάρτα USIM και στο δίκτυο. Εντούτοις, η γρήγορη επαναπιστοποίηση επαναχρησιμοποιεί τα κλειδιά που παράγονται από την προηγούμενη διαδικασία επικύρωσης. Τα πλεονεκτήματα της γρήγορης επαναπιστοποίηση είναι όχι μόνο να κερδηθεί χρόνος επεξεργασίας στο WLAN UE και τον διακομιστή AAA, αλλά και να μειωθεί η κατανάλωση ισχύος στο UE. Η χρήση της γρήγορης επαναπιστοποίηση εξαρτάται από τις πολιτικές του χειριστή.

Στο [24], αναλύεται ένας μηχανισμός πιστοποίησης για την απρόσκοπτη κινητικότητα μεταξύ 3GPP και WLAN, μέσω δοκιμών που βασίζονται στο USIM και παρουσιάζει αναλυτικά αποτελέσματα με τη μέτρηση και τη σύγκριση της καθυστέρησης της γρήγορης επαναπιστοποίησης και της πλήρους πιστοποίησης στο EAP-AKA.

4.3.3 WLAN 3GPP IP

Σε αντίθεση με την πρόσβαση WLAN Direct IP, στην οποία ο χρήστης αποκτά πρόσβαση στο Διαδίκτυο άμεσα, διαμέσου ενός WLAN-AN, στην περίπτωση της πρόσβασης WLAN 3GPP IP παρέχεται πρόσβαση στον χρήστη του WLAN διαμέσου του 3G PLMN. Πριν δοθεί πρόσβαση ο χρήστης πρέπει να ακολουθήσει έξι διακριτά βήματα όπως απεικονίζονται στην Εικόνα 4, τα οποία είναι:



Εικόνα 8. Διαδικασία πιστοποίησης 3GPP IP

1. *Αρχική πιστοποίηση*. Γίνεται αμοιβαία πιστοποίηση χρήστη-δικτύου χρησιμοποιώντας είτε το πρωτόκολλο EAP-SIM ή το EAP-AKA. Αυτό το βήμα επιτρέπει στον χρήστη να

αποκτήσει μια τοπική διεύθυνση IP, που καλείται διεύθυνση Transport IP και χρησιμοποιείται για πρόσβαση στο WLAN και στο PDG.

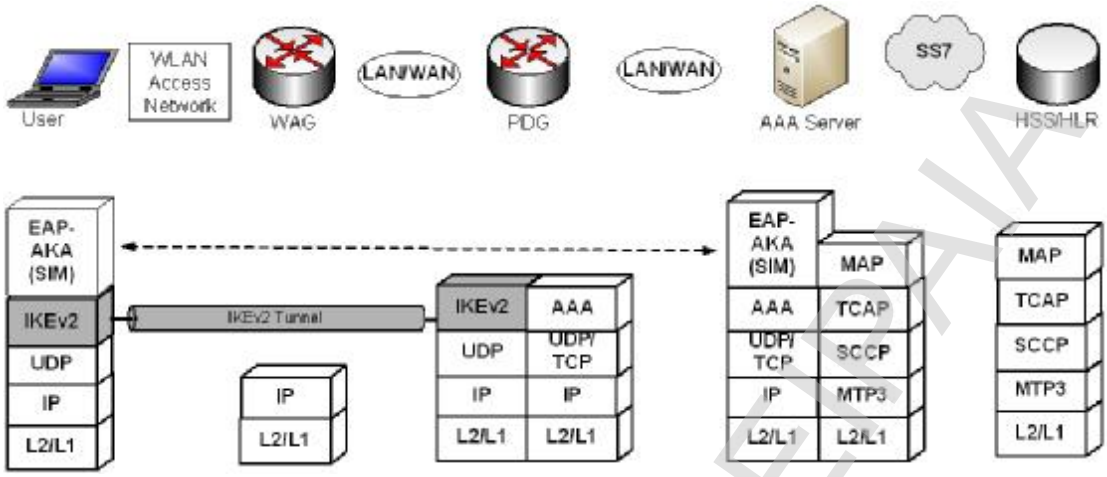
2. Μετά την εκτέλεση του EAP-SIM ή του EAP-AKA, ακολουθεί η τετραπλή χειραψία του 802.11i για την παροχή των κλειδιών συνόδου. Στη συνέχεια η επικοινωνία ανάμεσα στον χρήστη και στο ασύρματο AP κρυπτογραφείται χρησιμοποιώντας το πρωτόκολλο CCMP ή το TKIP.

3. Μετά την χειραψία του 802.11i, ο χρήστης επικοινωνεί με τον διακομιστή DHCP για να αποκτήσει την διεύθυνση Transport IP. Αυτή η τοπική διεύθυνση χρησιμοποιείται από τον χρήστη για την εκτέλεση του IKEv2 στο επόμενο βήμα

4. Ο χρήστης λαμβάνει την διεύθυνση IP του PDG χρησιμοποιώντας την ταυτότητα W-APN και το πρωτόκολλο DNS. Για αυτόν τον σκοπό ο χρήστης και το PDG συμμετέχουν σε έναν δεύτερο γύρο πιστοποίησης που συνδυάζει το IKEv2 και το EAP-SIM ή το EAP-AKA

5. *Δεύτερος γύρος πιστοποίησης*. Ο χρήστης και το PDG εκτελούν το πρωτόκολλο IKEv2, το οποίο ενσωματώνει το πρωτόκολλο EAP-SIM ή το EAP-AKA για την πιστοποίηση. Μετά την ολοκλήρωση της πιστοποίησης, ο χρήστης αποκτά μια καθολική διεύθυνση IP, που ονομάζεται Remote IP και χρησιμοποιείται για την πρόσβαση στις υπηρεσίες PS και στο Διαδίκτυο μέσω του 3G PLMN. Επιπρόσθετα η εκτέλεση του IKEv2 καταλήγει στην καθιέρωση ενός ζεύγους IPsec Security Associations (SA) ανάμεσα στον χρήστη και στο PDG, που χρησιμοποιούνται για την εγκατάσταση ενός IPsec VPN.

6. Το εγκατεστημένο IPsec VPN προστατεύει τα δεδομένα χρήστη που ανταλλάσσονται ανάμεσα στον χρήστη και στο PDG, εγγυώντας την πιστοποίηση της προέλευσης των δεδομένων και την ακεραιότητα τους



Εικόνα 9. Στοίβα πρωτοκόλλου πιστοποίησης 3GPP IP

Η Εικόνα 9 απεικονίζει την στοίβα πρωτοκόλλων που χρησιμοποιείται στην περίπτωση της πρόσβασης 3GPP IP για κάθε οντότητα που συμμετέχει στην διαδικασία πιστοποίησης. Το βασικό πρωτόκολλο πιστοποίησης είναι το EAP-SIM ή το EAP-AKA. Ο χρήστης ενσωματώνει μηνύματα EAP-SIM ή EAP-AKA μέσα στο IKEv2 και τα μεταβιβάζει στο PDG. Το PDG ενεργεί ως πελάτης AAA και μεταφέρει τα μηνύματα στον διακομιστή AAA χρησιμοποιώντας ένα AAA πρωτόκολλο. Ο διακομιστής AAA συμπεριλαμβάνει και την στοίβα πρωτοκόλλου MAP (Mobile Application Part) για να μπορεί να επικοινωνεί με το HSS/HLR.

4.3.4 QoS και Ασφάλεια

Σε αυτήν την ενότητα παρουσιάζουμε μια προσέγγιση σχετικά με την ασφάλεια και το QoS που προτείνεται στο [25]. Παρουσιάζεται μια αρχιτεκτονική συστήματος για την ασφάλεια και το QoS σε περιβάλλον B3G, που ενσωματώνει το QoS με τον μηχανισμό AAA. Δεδομένου ότι το κλασικό AAA δεν ταιριάζει για την κινητικότητα, το AAA του B3G χρειάζεται να είναι αποδοτικότερο και πιο εξελιγμένο. Συνεπώς εξετάζονται διάφορα ζητήματα QoS και ασφάλειας όπως:

- Προβλήματα βελτιστοποίησης δρομολόγησης ανάμεσα στο CN και το MN

- Πώς να υπάρχουν εγγυήσεις του QoS σε τυχόν καθυστερήσεις
- Πώς να ενσωματωθεί το QoS με το AAA.

Η αρχιτεκτονική που προτείνεται ονομάζεται SeaSoS και επιτρέπει την μεταβολή των ιδιοτήτων του δικτύου χρησιμοποιώντας δυναμικά **plugins**, ή παραμέτρους που μπορούν να επαναδιαμορφωθούν για να πραγματοποιείται η αλληλεπίδραση με ετερογενή δίκτυα όπως:

• Πρωτόκολλο QoS: RSVP + NSIS-QoS
• Πρωτόκολλο AAA: Diameter + COPS
• HMIPv6 + MIPv6

Η αρχιτεκτονική SeaSoS μπορεί επίσης να πραγματοποιήσει την απρόσκοπτη πρόσβαση (Seamless Access). Επίσης λόγω του ότι η αρχιτεκτονική SeaSoS εφαρμόζει το RSVP μπορεί να αποτρέψει επιθέσεις DoS.

4.3.5 Ασφάλεια στο Mobile IPv6

Στο [26] προτείνεται μια αρχιτεκτονική συστημάτων για ασφαλές κινητό IPv6 για δίκτυα B3G. Στο κινητό IPv6 όταν περιπλανάται το MN μακριά από το HN του, ο μηχανισμός ND ή το πρωτόκολλο DHCP δεσμεύει τη νέα διεύθυνση με την αποστολή του μηνύματος BU (Binding Update) στο HA.
Επιπλέον ο μηχανισμός RRP (Return Routability Procedure) είναι ευάλωτος σε επιθέσεις κατά μήκος της διαδρομής από το HA μέχρι το CN, όπου ένας κακόβουλος κόμβος μπορεί να στείλει πλαστά μηνύματα HoTI και CoTI. Ο επιτιθέμενος μπορεί να αποκτήσει το Kbm (Binding Management Key) και να στείλει πλαστό BU στο CN ή στο MN. Ως εκ τούτου το κινητό IPv6 σε ετερογενές δίκτυο θα υποστεί μια επίθεση πλαστοπροσωπίας (impersonation) ή επίθεση man-in-the-middle.
Για αυτό το λόγο προτείνεται μια αρχιτεκτονική συστημάτων για να επιλύσει αυτά τα ζητήματα ασφαλείας του κινητού IPv6 για B3G δίκτυα [26]. Οι λύσεις για τις επιθέσεις man-in-the-middle είναι:

- Το BU πρέπει να ενημερώνεται σε κάθε handoff

- σε κάθε διαδρομή, πρέπει να υιοθετείται το IPSec ή το ESP για την προστασία της διανομής των κλειδιών.

Κατά την αρχικοποίηση Kbm διανέμεται το MN και το CN μέσα στο σώμα του μηνύματος SIP 200 OK και ACK, αντί του RRP. Το Kbm μπορεί να παραχθεί από τον κεντρικό υπολογιστή AAA. Η διανομή των κλειδιών εξασφαλίζεται από το IPSec και το ESP ανάμεσα στον χρήστη SIP (MN και CN) και στο P-CSCF.

4.3.6 Αρχιτεκτονική ασφαλείας Trusted Computing

Στο B3G υπάρχουν μερικά τεχνολογικά ζητήματα όπως η παροχή μεγάλης ευελιξίας και κινητικότητας που κάνουν ακόμα πιο σύνθετο το πρόβλημα ασφάλειας. Στο [27] προτείνεται, μια αρχιτεκτονική ασφάλειας (Trusted Computing-Based Security Architecture)$_{για}$ το B3G που βασίζεται στο σχήμα PKBP. Έχουν προταθεί διάφορα πρωτόκολλα πιστοποίησης για το κινητό IP, τα οποία όμως δεν μπορούν να χρησιμοποιηθούν ως έχουν στο B3G, για τους παρακάτω λόγους:

• Το πρωτόκολλο που βασίζεται σε συμμετρικό κλειδί δεν μπορεί να λειτουργήσει λόγω της κακής κλιμάκωσης (scalability) του.

• Το πρωτόκολλο που βασίζεται σε δημόσιο κλειδί προκαλεί αύξηση στο υπολογιστικό φορτίο.

• Είναι αδύνατο να ληφθεί μια CA για τα ετερογενή δίκτυα στο B3G.

• Είναι πολύ δύσκολο για το ME να ελέγξει την εγκυρότητα του πιστοποιητικού δημόσιου κλειδιού του BS, διότι το ME και το BS ανήκουν συνήθως σε διαφορετική CA.

• Είναι δύσκολο να επιτευχθεί η αμοιβαία επικύρωση μεταξύ ME και του FA, και το ME είναι ευάλωτο και μπορεί να εξαπατηθεί από ένα πλαστό BS/FA.

Στην αρχιτεκτονική ασφάλειας που προτείνεται χρησιμοποιείται ένα ιεραρχικό μοντέλο εμπιστοσύνης. Κάθε ασύρματο δίκτυο έχει μια κεντρική CA (RCA) και τα διαφορετικά δίκτυα ενώνονται μεταξύ τους μέσω μιας γέφυρας CA (BCA). Κάθε CA χρησιμοποιεί το PKI και το πρωτόκολλο X.509. Η προτεινόμενη αυτή αρχιτεκτονική είναι μια εφικτή λύση για την παροχή ασφάλειας σε B3G.

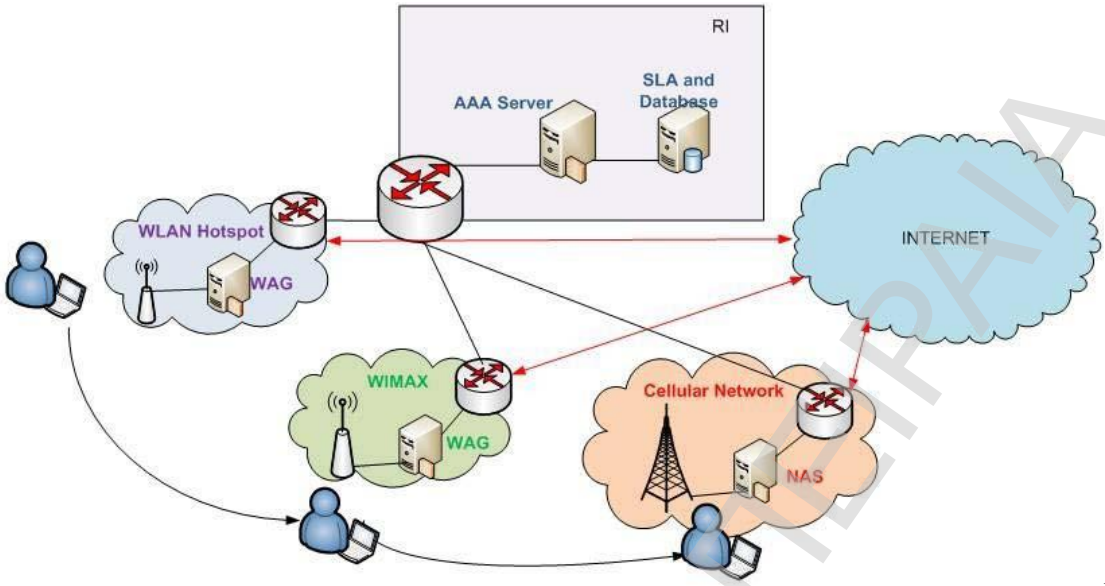
4.3.7 Ασφαλές Roaming μεταξύ δικτύων WLAN και WIMAX

Το πρότυπο IEEE 802.16 [28] είναι μια τεχνολογία που παρέχει ευρυζωνική ασύρματη πρόσβαση. Το εμπορικό όνομα του προτύπου IEEE 802.16 είναι «WiMAX» και αποτελεί μια ασύρματη τεχνολογία με σκοπό να καλύψει ευρείες γεωγραφικές περιοχές εξυπηρετώντας μεγάλους αριθμούς χρηστών σε χαμηλό κόστος. Η αρχική μελέτη έχει γίνει από το φόρουμ WiMAX για τη δημιουργία των μηχανισμών αλληλεπίδρασης με το 3GPP σύστημα. Το WLAN και το PLMN είναι ταξινομημένα βάσει δύο διαφορετικών μηχανισμών: (α) χαλαρής αλληλεπίδρασης και (β) στενά συνδεμένης αλληλεπίδρασης. Για την παροχή αλληλεπίδρασης διαμέσου της πιστοποίησης ασφαλείας σε ετερογενή δίκτυα, η διαχείριση κινητικότητας (mobility management) πρέπει να διατηρηθεί στα δίκτυα πρόσβασης.

Το roaming περιλαμβάνει την επιλογή δικτύου, την πιστοποίηση, την έγκριση και τις διευθετήσεις τιμολόγησης μεταξύ των χειριστών. Στο [27] προτείνεται μια λύση για το roaming και την μεταβίβαση (handover) χρησιμοποιώντας τη διαχείριση θέσης για την επιλογή του δικτύου με τη βοήθεια ενός ενδιάμεσου παρόχου, του αποκαλούμενου RI (Roaming Intermediatory). Ο RI ενεργεί όπως ένας μεσίτης στην αρχιτεκτονική RII μεταξύ του home και του visited δικτύου. Ο RI παρέχει διαχείριση κινητικότητας, τη μεταφορά context μεταξύ των παρόχων υπηρεσιών, την αρχιτεκτονική ασφάλειας για την πιστοποίηση και τις συσχετίσεις των χρηστών κατά το roaming, και τη διαχείριση παρουσίας (presence management). Στο RII οι παροχείς δικτύων δεν χρειάζεται να έχουν SLAs μεταξύ τους, αντ' αυτού παρέχουν roaming για τους ξένους χρήστες με τη βοήθεια της αρχιτεκτονικής RII.

Αρχιτεκτονική RII

Ο ρόλος της αρχιτεκτονικής RII είναι να παρασχεθεί ασφαλές roaming διαμέσου των ετερογενών δίκτυων. Η αρχιτεκτονική RII εισάγει το στοιχείο RI, το WAG στο WLAN, τα δίκτυα WIMAX και τον διακομιστή πρόσβασης δίκτυου NAS στα κυψελοειδή δίκτυα. Η αρχιτεκτονική RII ενσωματώνεται με τα δίκτυα παροχής υπηρεσιών όπως φαίνεται στην



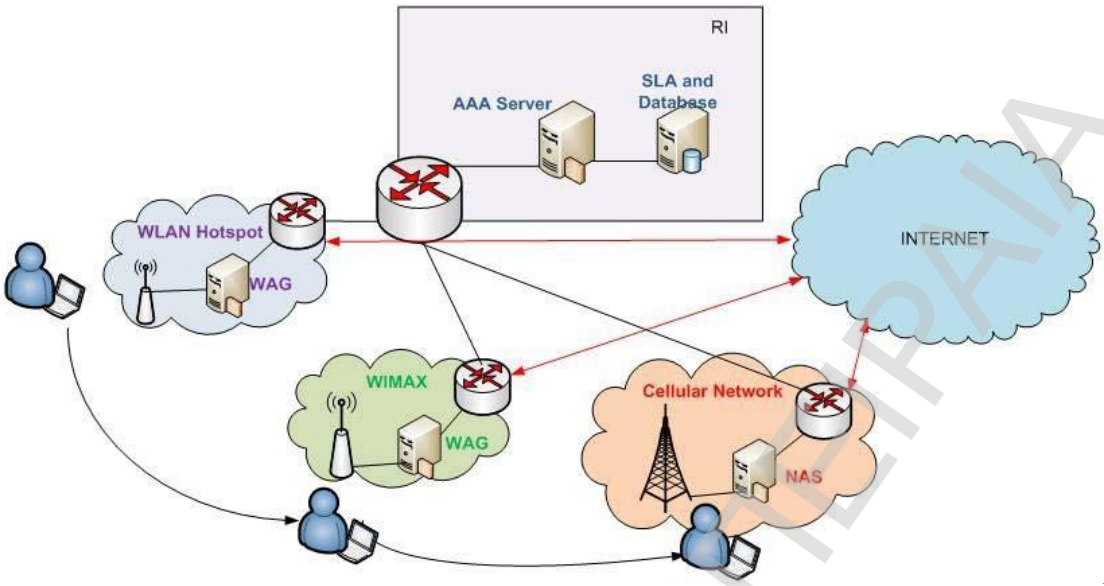
Εικόνα 10

Εικόνα 10.

Ο RI παρέχει την υποστήριξη για το roaming και τη διαχείριση κινητικότητας για τους χρήστες.

Το home δίκτυο και τα visited δίκτυα μεσολαβούν μέσω του RI για την παροχή πρόσβασης στους χρήστες. Εάν οι χειριστές θέλουν να παρέχουν υπηρεσία roaming στους χρήστες τους, δεν είναι απαραίτητο να έχουν SLA μεταξύ όλων των χειριστών, αντ' αυτού μπορούν να έχουν συμφωνία με το RI για να παρέχουν τις υπηρεσίες τους. Εάν οι χειριστές έχουν προηγούμενες συμφωνίες με κάποιον άλλο χειριστή, το roaming μπορεί να γίνει μέσω του WAG ή του NAS στο δίκτυο χειριστών.

Τα υποσυστήματα του RI είναι η διαχείριση παρουσίας (γεωπληροφοριες), διαχείριση πιστοποίησης, διαχείριση κινητικότητας, διαχείριση λογαριασμών, μονάδα πληρο-φοριών χειριστών (SLAs και διαχείριση πολιτικής) και μεταφοράς context.



Εικόνα 10. Η αρχιτεκτονική RII

- Η διαχείριση παρουσίας είναι το υποσύστημα του RI που χρησιμοποιείται για τη διαχείριση θέσης και είναι εξοπλισμένο με σύστημα GIS με την χαρτογράφηση των περιοχών κάλυψης του κυψελωτού δικτύου. Εάν υπάρχουν οποιαδήποτε ερωτήματα από τα δίκτυα χειριστών σχετικά με τα διαθέσιμα δίκτυα σε μια συγκεκριμένη περιοχή, τότε αυτό το υποσύστημα απαντά παρέχοντας τις πληροφορίες κάλυψης του δικτύου. Εάν δεν υπάρχει καμία σχετικά πληροφορία διαθέσιμη σε αυτό το υποσύστημα τότε προωθεί τις ερωτήσεις σε όλους τους άλλους χειριστές για να απαντήσει με την σειρά του στο αρχικό ερώτημα.

- Η μονάδα διαχείρισης λογαριασμών (Accounting Unit) εξετάζει τη λογιστική των υπηρεσιών roaming που χρησιμοποιούνται από τους χειριστές, στα άλλα δίκτυα, για τους χρήστες τους.

- Η μονάδα διαχείρισης κινητικότητας χρησιμοποιείται για τις αποφάσεις μεταβίβασης και για την υποστήριξη των χρηστών στα δίκτυα πρόσβασης.

- Η μονάδα μεταφοράς context (Context Transfer) αναλαμβάνει την ασφάλεια της μεταφοράς context .

Το WAG και το NAS παρέχουν την υποστήριξη για την πιστοποίηση των χρηστών, τη διαχείριση κινητικότητας, την ενημέρωση θέσης, τη χαρτογράφηση GIS, τις πληρο-φορίες κάλυψης δικτύου και τη βάση δεδομένων των χρηστών στα δίκτυα πρόσβασης. Το WAG περιέχει τη μονάδα διαχείρισης τοποθεσίας (Location Management unit), τη μονάδα πιστοποίησης, τη μονάδα διαχείρισης κινητικότητας και τη μονάδα μεταφοράς context για την επικοινωνία μεταξύ WAG και με το RI.

Στη μονάδα πιστοποίησης, στην οποία οι χρήστες πιστοποιούνται στο σύστημα, το WAG λαμβάνει το αίτημα για τις πιστοποιήσεις και τις επαναπιστοποιήσεις. Το τερματικό πιστοποιείται σύμφωνα με τη χρήση των μηχανισμών ασφάλειάς των δικτύων πρόσβασης. Για ένα αίτημα πιστοποίησης από άλλα δίκτυα, τα κλειδιά που παράγονται στο ξεκίνημα του τερματικού, στέλνονται στα άλλα WAG και στο RI με τη βοήθεια της μεταφοράς context για να γίνουν οι πιστοποιήσεις με χαμηλή καθυστέρηση.

Στην μονάδα διαχείρισης τοποθεσίας, βρίσκονται οι θέσεις των χρηστών και γεωπληροφορίες GIS με την αντίστοιχη κάλυψη πρόσβασης. Εάν υπάρχουν οποια-δήποτε ερωτήματα από το τερματικό σχετικά με την παρούσα θέση του, αυτή η μονάδα βρίσκει τη διαθεσιμότητα των δικτύων και απαντά στο τερματικό.

Η μονάδα διαχείρισης κινητικότητας, παρέχει υποστήριξη στα τερματικά κατά τη διάρκεια της μεταβίβασης και του roaming για να επιλέξουν το καλύτερο δίκτυο βάσει της πολιτικής του χρήστη, του QoS, του κόστους και των SLA με τους άλλους χειριστές.

4.3.8 Μηχανισμοί ασφαλούς πρόσβασης στο δίκτυο WLAN

Το IEEE 802.1X είναι ένα port-based πρότυπο ελέγχου πρόσβασης δίκτυου που παρέχει διαδικασίες ισχυρής πιστοποίησης και έλεγχο πρόσβασης για δίκτυα που βασίζονται στο πρότυπο 802.11. Οι διάφορες μέθοδοι πιστοποίησης όπως τα ψηφιακά πιστοποιητικά, οι έξυπνες κάρτες και οι κωδικοί πρόσβασης μπορούν να χρησιμοποιηθούν για να παρέχουν πληροφορίες επικύρωσης για την πιστοποίηση. Ο πιο κοινός τύπος διακομιστή πιστοποίησης (Authentication Server, AS) είναι ο RADIUS (Remote Authentication Dial-In User Service) [29]. Η διαδικασία πιστοποίησης στο 802.1X χρησιμοποιεί το πρωτόκολλο EAP για να μεταβιβάσει τις πληροφορίες επικύρωσης μεταξύ του τερματικού και του AS. Το EAP δημιουργεί μια σύνοδο με τον AS έτσι ώστε το τερματικό να διαβιβάσει τις πληροφορίες πιστοποίησης.

Η σύνοδος EAP επιτρέπει στο τερματικό μια περιορισμένη ασύρματη πρόσβαση στο δίκτυο μόνο για σκοπούς πιστοποίησης. Μόλις η πιστοποίηση ολοκληρωθεί, η σύνοδος τερματίζεται και στο ασύρματο τερματικό αποκτά πρόσβαση. Το 802.1X υποστηρίζει μηχανισμούς όπως είναι το MD5, το TLS (Transport Layer Security), το PEAP (Protected Extensible Authentication Protocol), το EAP-SIM και το EAP-AKA. Η επιλογή δικτύου γίνεται ως εξής: ο πελάτης WLAN επιλέγει ένα δίκτυο πρόσβασης και στέλνει ένα Decorated NAI του RI ή πληροφορίες του home δικτύου στο πεδίο Type-Data του EAP-Identity Response ως απάντηση για το πακέτο EAP-request που στέλνεται από το δίκτυο πρόσβασης .

Το AP του ξένου δικτύου ενσωματώνει το EAP-Response μέσα σε ένα EAP-Message και το στέλνει στον διακομιστή RADIUS μέσα σε ένα πακέτο RADIUS Access-Request. Αντιγράφει επίσης το περιεχόμενο του πεδίου Type-Data του EAP-Response με το decorated NAI, στην ιδιότητα (attribute) User-Name. Όταν ο διακομιστής RADIUS λάβει ένα πακέτο RADIUS Access-Request, που περιέχει ένα decorated NAI, το οποίο δεν διευκρινίζει ένα δίκτυο πρόσβασης που αναγνωρίζεται από το FN σαν τον επόμενο κομβο-hop για την δρομολόγηση του πακέτου RADIUS, ο διακομιστής RADIUS FN πρέπει να δρομολογήσει το πακέτο RADIUS στον RI και ο RI προωθεί το πακέτο RADIUS στο home δίκτυο του χρήστη.

4.3.9 Μηχανισμοί ασφαλούς πρόσβασης στο δίκτυο WIMAX

Η αρχιτεκτονική ασφάλειας 802.16 διαιρείται σε δύο στρώματα. Το πρώτο στρώμα παρέχει ενθυλάκωση για την πρόσβαση δεδομένων στα δίκτυα 802.16. Το δεύτερο είναι ένα πρωτόκολλο διαχείρισης κλειδιών (PKM) που παρέχει την ασφαλή διανομή των κλειδιών μεταξύ του BS και του τερματικού. Το PKM υποστηρίζει και την αμοιβαία πιστοποίηση αλλά και τη μονομερή. Το PKM χρησιμοποιεί ψηφιακά πιστοποιητικά EAP ή X.509 μαζί με RSA ή μια ακολουθία που ξεκινά με RSA και συνεχίζει με το EAP. Ένα BS πιστοποιεί ένα τερματικό-πελάτη κατά τη διάρκεια της αρχικής διαδικασίας εξουσιοδότησης. Κάθε τερματικό παρουσιάζει τα πιστοποιητικά του, τα οποία είναι ένα μοναδικό ψηφιακό πιστοποιητικό X.509 που εκδίδεται από τον κατασκευαστή του τερματικού στην περίπτωση πιστοποίησης RSA ή ένα πιστοποιητικό που έχει ορίσει ο χειριστής στην περίπτωση πιστοποίησης EAP. Όπως στο WLAN έτσι και το WIMAX χρησιμοποιεί EAP NAI για την πιστοποίηση στα δίκτυα WIMAX.

4.4 Αποτίμησης της αρχιτεκτονικής ασφαλείας σε B3G

Σε αυτό το κεφάλαιο γίνεται αποτίμηση των τεχνικών ασφαλείας που χρησιμοποιούνται στις δυο διαφορετικές περιπτώσεις δικτύωσης που συνδυάζουν τις τεχνολογίες 3G και WLAN. Η αποτίμηση γίνεται βάσει των παρεχόμενων υπηρεσιών ασφάλειας, καθώς επίσης και βάσει θεμάτων λειτουργικότητας και απόδοσης που σχετίζονται με την χρήση τους [23].

4.4.1 Αποτίμηση EAP-SIM

Παρόλο που το EAP-SIM σχεδιάστηκε σαν ένα εξελιγμένο πρωτόκολλο πιστοποίησης, δεν ικανοποιεί τους στόχους ασφαλείας που διακηρύττει. Ένα βασικό μειονέκτημα της διαδικασίας πιστοποίησης του EAP-SIM σχετίζεται με το γεγονός ότι οι σύνοδοι του δεν είναι ανεξάρτητες [22]. Συγκεκριμένα, εάν κάποιες από τις τριπλέτες πιστοποίησης του χρήστη εκτεθούν σε τρίτους, τότε κάποιος μπορεί να τις χρησιμοποιήσει για να πιστοποιηθεί στον χρήστη σαν να είναι ένα έγκυρο δίκτυο. Οι τρόποι με τους οποίους κάποιος τρίτος μπορεί να αποκτήσει τις τριπλέτες πιστοποίησης είναι:

(α) έχοντας φυσική πρόσβαση στην κάρτα SIM του χρήστη,

(β) χρησιμοποιώντας κακόβουλο λογισμικό που πραγματοποιεί επίθεση στην πλατφόρμα του χρήστη,

(γ) πραγματοποιώντας επιθέσεις στο δίκτυο GSM/GPRS (κάνοντας την υπόθεση ότι χρησιμοποιούνται οι ίδιες τριπλέτες πιστοποίησης και για την πρόσβαση στο GSM/GPRS και στο WLAN)

(δ) αποκτώντας πρόσβαση στην επικοινωνία ανάμεσα στο AuC και στον διακομιστή AAA που ανταλλάσουν πληροφορίες πιστοποίησης.

Αποκτώντας τις τριπλέτες πιστοποίησης κάποιος μπορεί να παριστάνει ένα έγκυρο δίκτυο και να υπολογίζει έγκυρα κλειδιά. Δηλαδή μπορεί να υπολογίζει μια έγκυρη τιμή $MAC_{διακομιστή}$ και αντίστοιχα να δημιουργεί το κλειδί K_auth. Βασιζόμενος στην τιμή $MAC_{διακομιστή}$ που θα λάβει

ο χρήστης, πιστοποιεί τον επιτιθέμενο σαν ένα γνήσιο και έγκυρο δίκτυο. Παρόλο που το EAP-SIM προστάζει την χρήση νέων τριπλετών πιστοποίησης, δεν υπάρχει μηχανισμός που να επιτρέπει στον χρήστη να ελέγχει εάν οι τριπλέτες, που έλαβε από τον διακομιστή AAA, είναι καινούργιες. Ο επιτιθέμενος μπορεί να χρησιμοποιεί τις τριπλέτες για όσο διάστημα το μυστικό κλειδί Ki παραμένει το ίδιο.

Εκτός από αυτήν την σημαντική αδυναμία, υπάρχουν και άλλοι τρόποι που κάποιος θα μπορούσε να εκμεταλλευτεί για να πραγματοποιήσει μια επίθεση στο EAP-SIM. Για παράδειγμα, ο χρήστης είναι υποχρεωμένος να αποστείλει την μόνιμη ταυτότητα IMSI χωρίς κρυπτογράφηση κατά την πρώτη φορά που συνδέεται με τον διακομιστή πιστοποίησης. Έτσι μπορεί να εκτεθεί η ταυτότητα του χρήστη μιας και κάποιος μπορεί να την υποκλέψει. Επιπρόσθετα, πολλά από τα μηνύματα του EAP-SIM (π.χ. EAP-Request/Notification, EAP-Response/Notification, EAP-Success και EAP-Failure) ανταλλάσσονται απροστάτευτα δίνοντας την δυνατότητα στον επιτιθέμενο να στείλει ψευδείς ειδοποιήσεις και έτσι να πραγματοποιήσει επιθέσεις Denial of Service παραπλανώντας τους συμμετέχοντες.

Μια λύση που ενισχύει το επίπεδο ασφαλείας του EAP-SIM, είναι η χρήση ειδικών RAND [3]. Βάσει αυτής της λύσης, το δίκτυο παραγάγει ειδικές τριπλέτες πιστοποίησης οι οποίες χρησιμοποιούνται μόνο για την πιστοποίηση στο EAP-SIM και όχι για το GSM/GPRS. Σε μια τέτοια τριπλέτα, η παράμετρος RAND εμπεριέχει ένα συγκεκριμένο κρυπτογραφικό στοιχείο που προσδιορίζει ότι η συγκεκριμένη τριπλέτα είναι σχεδιασμένη για πιστοποίηση EAP-SIM. Έτσι δεν μπορεί να χρησιμοποιηθεί από κάποιον μια τριπλέτα του GSM/GPRS στο EAP-SIM. Παρόλαυτα αυτή η λύση είναι σύνθετη και δεν μπορεί να εφαρμοστεί εύκολα, διότι απαιτεί αλλαγές στις υπάρχουσες υποδομές του δικτύου GSM/GPRS.

4.4.2 Αποτίμηση του EAP-AKA

Το EAP-AKA, που βασίζεται στην διαδικασία πιστοποίησης και συμφωνίας κλειδιού του UMTS, εξουδετερώνει τις επιθέσεις πλαστής ταυτότητας χρησιμοποιώντας έναν μηχανισμό που προστατεύει από επιθέσεις-replay. Αυτός ο μηχανισμός εμπεριέχει τον υπολογισμό και την επαλήθευση μιας ειδικής τιμής AUTN που ονομάζεται σύμβολο πιστοποίησης [8]. Εάν κάποιος επιτιθέμενος αποκτήσει ένα διάνυσμα πιστοποίησης, δεν μπορεί να το ξαναχρησιμοποιήσει, διότι η επαλήθευση AUTN θα αποτύχει. Σε περίπτωση που προσπαθήσει να ξαναυπολογίσει

ένα έγκυρο AUTN, θα αποτύχει και πάλι μιας και ο υπολογισμός αυτός απαιτεί το μυστικό κλειδί K, το οποίο δεν μπορεί να αποκτηθεί μιας και είναι κρυπτογραφημένο.
Παρόλο που το EAP-AKA ενισχύει το επίπεδο ασφάλειας στα δίκτυα B3G, παρουσιάζει κάποιες αδυναμίες όμοιες με αυτές στο EAP-SIM. Συγκεκριμένα το πρωτόκολλο EAP-AKA δεν προσφέρει προστασία ταυτότητας, μιας και η ταυτότητα IMSI μπορεί να μεταβιβαστεί χωρίς κρυπτογράφηση. Ο επιτιθέμενος παριστάνοντας έναν έγκυρο διακομιστή AAA, μπορεί να εξαναγκάσει τον χρήστη να στείλει την IMSI του. Επιπλέον, πολλά από τα μηνύματα του EAP-AKA (πχ, EAP-Request/Notification, EAP-Response/Notification, EAP-Success και EAP-Failure) ανταλλάσσονται απροστάτευτα.

4.4.3 Αποτίμηση του IEEE 802.11i

Το πρότυπο 802.11i, που παρέχει προηγμένες υπηρεσίες ασφάλειας στα δεδομένα που μεταφέρονται ασύρματα, εξουδετερώνει τα κενά ασφάλειας του προγόνου του, WEP. Εντούτοις, η εγκαθίδρυση αυτού του προτύπου εγείρει ζητήματα κατανάλωσης ενέργειας και συμβατότητας.

Όσον αφορά τη συμβατότητα, το κύριο ενδιαφέρον βρίσκεται στην απρόσκοπτη συνεργασία μεταξύ των νέων αναδυόμενων συστημάτων που υποστηρίζουν το πλαίσιο ασφάλειας 802.11i με τα παλαιότερα συστήματα που δεν το υποστηρίζουν. Η παλαιότερη υποδομή WLAN δεν μπορεί να ενσωματώσει εύκολα το πλαίσιο ασφάλειας 802.11i, δεδομένου ότι πρέπει να ενσωματώσει επιπρόσθετο λογισμικό και υλικό. Οι σημαντικότερες βελτιώσεις πρέπει να γίνουν στα παλαιά ασύρματα AP τα οποία πρέπει να υλοποιήσουν τον αλγόριθμο AES που μπορεί να απαιτήσει έναν πρόσθετο συνεπεξεργαστή. Κατά συνέπεια, για την ευρεία εγκατάσταση του 802.11i, η υπάρχουσα υποδομή δικτύων WLAN πρέπει να ενισχυθεί και ενδεχομένως να πρέπει να αντικατασταθούν τα παλαιότερα ασύρματα AP.

Επιπλέον, η κατανάλωση ενέργειας αποτελεί εμπόδιο για την αποδοχή 802.11i από τους χρήστες και από την εγκατάσταση του σε WLAN. Το βασικό ζήτημα έχει να κάνει με την περιορισμένη ισχύ των μπαταριών των κινητών συσκευών, δεδομένου ότι το 802.11i δεν θεωρείται ένα ενεργειακά αποδοτικό πρωτόκολλο. Αντίθετα τα μηνύματα που ανταλλάσσονται κατά τη διάρκεια των χειραψιών του 802.11i καθώς επίσης και οι κρυπτογραφικοί αλγόριθμοι

που σχετίζονται με αυτές τις χειραψίες, καταναλώνουν σημαντική ενέργεια. Στο [21] προσδιορίζονται τέτοια ζητήματα κατανάλωσης ενέργειας καθώς επίσης παρουσιάζονται μέθοδοι για την μέτρηση της κατανάλωσης ενέργειας των κρυπτογραφικών αλγορίθμων και προτείνονται λύσεις για να μειωθεί η κατανάλωση ενέργειας των πρωτοκόλλων ασφάλειας.

Ένα άλλο ζήτημα εγκατάστασης του 802.11i συσχετίζεται με το γεγονός ότι παρέχει τις υπηρεσίες ασφάλειας μόνο μεταξύ των χρηστών και των AP, αφήνοντας απροστάτευτη την επικοινωνία μεταξύ AP και NAS. Επομένως πρέπει να δοθεί ιδιαίτερη προσοχή στη φυσική ασφάλεια των συνδέσεων που συνδέουν AP με NAS, δεδομένου ότι μπορούν να μεταβιβάσουν τα δεδομένα χωρίς κρυπτογράφηση. Επιπλέον ιδιαίτερη προσοχή πρέπει να δοθεί στη φυσική ασφάλεια των ασύρματων AP τα οποία κατανέμονται στη γεωγραφική περιοχή που καλύπτεται από το WLAN-AN. Εάν ένα AP δεν προστατεύεται επαρκώς, τότε ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε αυτό και συνεπώς στις πληροφορίες ασφάλειας (δηλ., στα κλειδιά συνόδου) που αυτό περιέχει. Λαμβάνοντας τις κρίσιμες αυτές πληροφορίες ασφάλειας, ο επιτιθέμενος μπορεί να εκτελέσει διάφορες επιθέσεις (όπως κοινοποίηση των ανταλλαγμένων δεδομένων, denial of service, κ.λ.π), οι οποίες υποβιβάζουν το επίπεδο ασφάλειας που παρέχεται στους χρήστες.

Πρόσφατα, έχει προταθεί μια λύση για την παραπάνω αδυναμία ασφάλειας του 802.11i [9], η οποία εγκαθιστά ένα VPN μεταξύ του χρήστη και του NAS ενός WLAN. Το VPN, που είναι βασισμένο σε IPsec, προστατεύει τα δεδομένα που ανταλλάσσονται όχι μόνο στην ασύρματη διεπαφή (δηλ., μεταξύ του χρήστη και του AP), αλλά και στην ενσύρματη σύνδεση μεταξύ του AP και του NAS. Επιπλέον, δεδομένου ότι το NAS είναι ένα κεντρικό τμήμα της υποδομής του WLAN, έχει υψηλότερο επίπεδο φυσικής ασφάλειας σε σχέση με τα ασύρματα AP. Κατά συνέπεια, είναι προτιμότερο να αποθηκεύονται τα κλειδιά κρυπτογράφησης σε αυτό και να παρέχει υπηρεσίες ασφάλειας σε ένα WLAN, δεδομένου ότι ένας επιτιθέμενος δεν μπορεί να έχει φυσική πρόσβαση σε αυτό. Το προτεινόμενο σύστημα ασφάλειας μπορεί να ενσωματωθεί εύκολα στην υπάρχουσα υποδομή WLAN, και απαιτεί βελτιώσεις στους χρήστες και στο NAS, οι οποίες πρέπει να ενσωματώσουν το κατάλληλο λογισμικό IPsec.

4.4.4 Αποτίμηση ασφαλείας στην πρόσβαση 3GPP IP

Διάφορα ζητήματα απόδοσης στο σενάριο πρόσβασης 3GPP IP μπορούν να έχουν αρνητική επίδραση στην ποιότητα της υπηρεσίας (quality of service) που προσφέρεται στους τελικούς χρήστες. Πιο συγκεκριμένα, στο σενάριο πρόσβασης 3GPP IP, ο χρήστης μπορεί να έχει μεγάλες καθυστερήσεις κατά τη διάρκεια της πιστοποίησης, δεδομένου ότι πρέπει να εκτελέσει δύο χωριστά βήματα πιστοποίησης. Στο αρχικό βήμα πιστοποίησης, ο χρήστης εκτελεί το EAP-SIM ή το EAP-AKA για να λάβει τη διεύθυνση transport IP. Κατόπιν, στον δεύτερο γύρο πιστοποίησης ο χρήστης εκτελεί το EAP-SIM ή το EAP-AKA ακόμα μια φορά, το οποίο ενθυλακώνεται σε μηνύματα IKEv2, για να εγκαταστήσει ένα VPN tunnel μεταξύ του και του PDG. Επομένως, αυτή η διπλή εκτέλεση του EAP-SIM ή EAP-AKA που συνδυάζεται με τον φόρτο που προσθέτει το IKEv2, μπορεί να προκαλέσει καθυστερήσεις στην πιστοποίηση του χρήστη και να καταναλώσει τους λιγοστούς πόρους του δικτύου.

Σε περιπτώσεις που το PDG εμπιστεύεται το δίκτυο WLAN, η πρώτη εκτέλεση EAP-SIM ή EAP-AKA μπορεί να παραλειφθεί επιταχύνοντας έτσι τη διαδικασία πιστοποίησης. Εντούτοις αυτή η πολιτική παρουσιάζει νέους κινδύνους και απειλές ασφάλειας. Εάν το πρώτο βήμα πιστοποίησης παραλείπεται, τότε ένας επιτιθέμενος θα μπορούσε να λάβει μια διεύθυνση IP από το δίκτυο WLAN χωρίς πιστοποίηση. Χρησιμοποιώντας αυτήν την διεύθυνση IP μπορεί είτε να εκτελέσει επιθέσεις flooding στο PDG είτε bandwidth επιθέσεις στην ασύρματη διεπαφή του WLAN. Αν και το IKEv2 χρησιμοποιεί cookies για να προστατεύσει το δίκτυο από επιθέσεις flooding, αυτός ο μηχανισμός δεν μπορεί να παρέχει ένα επαρκές επίπεδο προστασίας. Δεδομένου ότι οι ανωτέρω επιθέσεις μπορούν να μειώσουν σημαντικά την ποιότητα της υπηρεσίας που παρέχεται από τα δίκτυα B3G, η προαναφερθείσα πολιτική πρέπει να εξεταστεί προσεκτικά πριν εφαρμοστεί.

Τέλος, η απόδοση στην περίπτωση πρόσβασης WLAN 3GPP IP στην μεταβίβαση δεδομένων μπορεί να μειωθεί, λόγω της χρήσης του IPsec. Συγκεκριμένα, το πρωτόκολλο IPsec αυξάνει τη χρησιμοποίηση εύρους ζώνης λόγω της αύξησης στο μέγεθος των πακέτων. Επιπλέον, η λειτουργικότητα IPsec προσθέτει υπολογιστικό κόστος που σχετίζεται με τη μνήμη που απαιτείται από τον κώδικα που χρησιμοποιεί το IPsec, τον αριθμό μηνυμάτων που ανταλλάσσονται, και τον υπολογιστικό χρόνο της κρυπτογράφησης και της αποκρυπτογράφησης, τα οποία προστίθενται ανα πακέτο.

Αναφορές κεφαλαίου

[1] http://www.enthesis.net/

[2] 3GPP TS 33.234 (v7.2.0), "*3G security; WLAN interworking security; System description*", Release 7, Sep. 2006.

[3] 3GPP Tdoc S3-0304, "*Cipher Key Separation or A/Gb security enhancements*", SA3#29 Jul. 2003.

[4] 3GPP TS 23.234 (v7.3.0), "*3GPP System to WLAN Interworking; System description*", Release 7, Sep. 2006.

[5] 3GPP TS 22.100 (v3.7.0), "*UMTS Phase 1 Release '99*", Oct. 2001.

[6] B.Aboba, M.Beadles, "*The Network Access Identifier*", RFC 2486, Jan. 1999

[7] B. Aboba, L. Blunk, J. Vollbrecht,J. Carlson, H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004

[8] C. Xenakis, L. Merakos, "*Security in third Generation Mobile Networks*", Computer Communications, Elsevier Science, Vol.27, No. 7, pp 638-650, May 2004.

[9] C. Ntantogian, C. Xenakis, L. Merakos, "*An Enhanced EAP-SIM Authentication Scheme for Securing WLAN*", 15th IST Mobile & Wireless Communications, Myconos, Greece, Jun. 2006.

[10] C. Laat, G .Gross, L.Gommans, J.Vollbrecht, D. Spence, "*Generic AAA Architecture*", RFC 2903, Aug. 2000.

[11] C. Kaufman, "*The Internet Key Exchange (IKEv2) Protocol*", RFC 4306, Dec. 2005.

[12] D. Stanley, J. Walker, B. Aboba, "Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs", March 2005

[13] D. Eastlake, P. Jones, "*US Secure Hash Algorithm 1 (SHA1)*", RFC 3174, Sep. 2001.

[14] ETSI TS 100 922 (v7.1.1), "*Subscriber Identity Modules (SIM) Functional characteristics*", Jul. 1999.

[15] H. Haverinen, J. Saloway "*EAP-SIM Authentication*", RFC 4186, Jan. 2006.

[16] H.Krawczyk, M.Bellare, R.Canetti, "*HMAC: Keyed-Hashing for Message Authentication*", RFC 2104, Feb. 1997

[17] IEEE Std 802.11i, "*Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements*", 2004.

[18] IEEE Std 802.11X, "*Port Based Network Access Control*", 2004.

[19] J. Arkko, H. Haverinen, "*EAP-AKA Authentication*", RFC 4187, Jan. 2006.

[20] N.Borisov, I.Goldberg, D.Wagner, "*Intercepting Mobile Communications: The Insecurity of 802.11*", 7th ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), Rome, Italy, Jul. 2001.

[21] P. Prasithsangaree, P. Krishnamurthy, "*On a Framework for Energy-Efficient Security Protocols in Wireless Networks*", Computer Communications, Elsevier Science, Vol. 27, No.17, pp. 1716-1729, Nov. 2004.

[22] S.Patel, "*Analysis of EAP-SIM Session Keys Agreement*", Lucent Technologies.

[23] Xenakis C., Ntantogian C., "*Security Architectures for B3G Mobile Networks*".

[24] Hyeyeon Kwon, Kyung-yul Cheon, Kwang-hyun Roh, «*USIM based Authentication Test-bed For UMTS-WLAN Handover*»

[25] Xiaoming Fu, Dieter Hogrefe, Sathya Narayanan, Rene Soltwish, "Qos and Security in 4G Networks," Proceedings of the first annual global mobile congress, Shanhai, China, Oct. 2004.

[26] D. Celentano, A. Fresa; M. Longo, F. Postiglione, A.L. Robustelli, *"Secure Mobile IPv6 for B3G Network",* SoftCOM 2006. International Conference on Software in Telecommunications and Computer Networks, PP. 331–335, Sept. 2006.

[27] Vamsi Krishna Gondi and Nazim Agoulmine, «Secured Roaming Over WLAN and WIMAX Networks».

[28] IEEE 802.16-2001, *"IEEE Standard for Local and Metropoli-tan Area Networks -Part 16: Air Interface for FixedBroadband Wireless Access Systems",* Apr. 8, 2002

[29] C. Rigney et.al, *"Remote Authentication Dial In User Service (RADIUS)",* RFC 2865.

Κεφάλαιο 5

Συμπεράσματα

Σε αυτήν την εργασία παρουσιάσαμε και αναλύσαμε θέματα σχεδίασης και ασφάλειας σχετικά με τα δίκτυα κινητής τηλεφωνίας UMTS και B3G. Αρχικά παρουσιάστηκαν τα πλεονεκτήματα των δικτύων UMTS, όπως είναι για παράδειγμα οι αυξημένοι ρυθμοί μετάδοσης δεδομένων και η υποστήριξη σύγχρονων μεθόδων ασφάλειας. Στην συνέχεια παρουσιάστηκε η αρχιτεκτονική του UMTS και αναλύθηκε η ασφάλειά του.

Η ασφάλεια UMTS διατήρησε, ως ένα βαθμό, τα ισχυρά χαρακτηριστικά ασφάλειας του GSM. Παρόλαυτα, τα προβλήματα ασφαλείας που εμφανίζονται σε έναν κόμβο που είναι συνδεδεμένος στο Internet ισχύουν αντίστοιχα και για έναν κόμβο που βρίσκεται σε περιβάλλον 3G. Οι προδιαγραφές ασφαλείας στο UMTS χωρίζονται στις εξής ομάδες χαρακτηριστικών ασφάλειας για την αποτελεσματικότερη κάλυψη των προβλημάτων ασφαλείας:

- Ασφάλεια πρόσβασης στο δίκτυο.
- Ασφάλεια περιοχής δικτύου.
- Ασφάλεια περιοχής χρηστών.
- Ασφάλεια περιοχής εφαρμογής.

Κατά την σχεδίαση του UMTS έχει ληφθεί υπόψη και η δυνατότητα νόμιμης υποκλοπής. Παρουσιάστηκαν οι υπηρεσίες και οι μέθοδοι που υποστηρίζουν την νόμιμη υποκλοπή σε περιβάλλον 3G καθώς και οι πιθανές επιπλοκές. Παρόλαυτα παραμένουν κάποια θέματα σχετικά με την νόμιμη υποκλοπή όπως είναι η υποστήριξη ποικιλόμορφων υπηρεσιών που παρέχουν οι διαφορετικές τεχνολογίες των παρόχων.

Τέλος, παρουσιάστηκε η γενική αρχιτεκτονική του διάδοχου του UMTS, του B3G και έγινε ανάλυση των τεχνικών ασφάλειας που χρησιμοποιούνται στις δυο διαφορετικές περιπτώσεις δικτύωσης που συνδυάζουν τις τεχνολογίες 3G και WLAN. Η αποτίμηση έγινε βάσει των παρεχόμενων υπηρεσιών ασφάλειας, καθώς επίσης και βάσει θεμάτων λειτουργικότητας και απόδοσης.