Ασφάλεια Κινητών και Ασύρματων Δικτύων Νέας Γενιάς

Ασφάλεια στο Δίκτυο UMTS

Γεώργιος Καρόπουλος
Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Αθηνών

Universal Mobile Telecommunication System (UMTS) /1

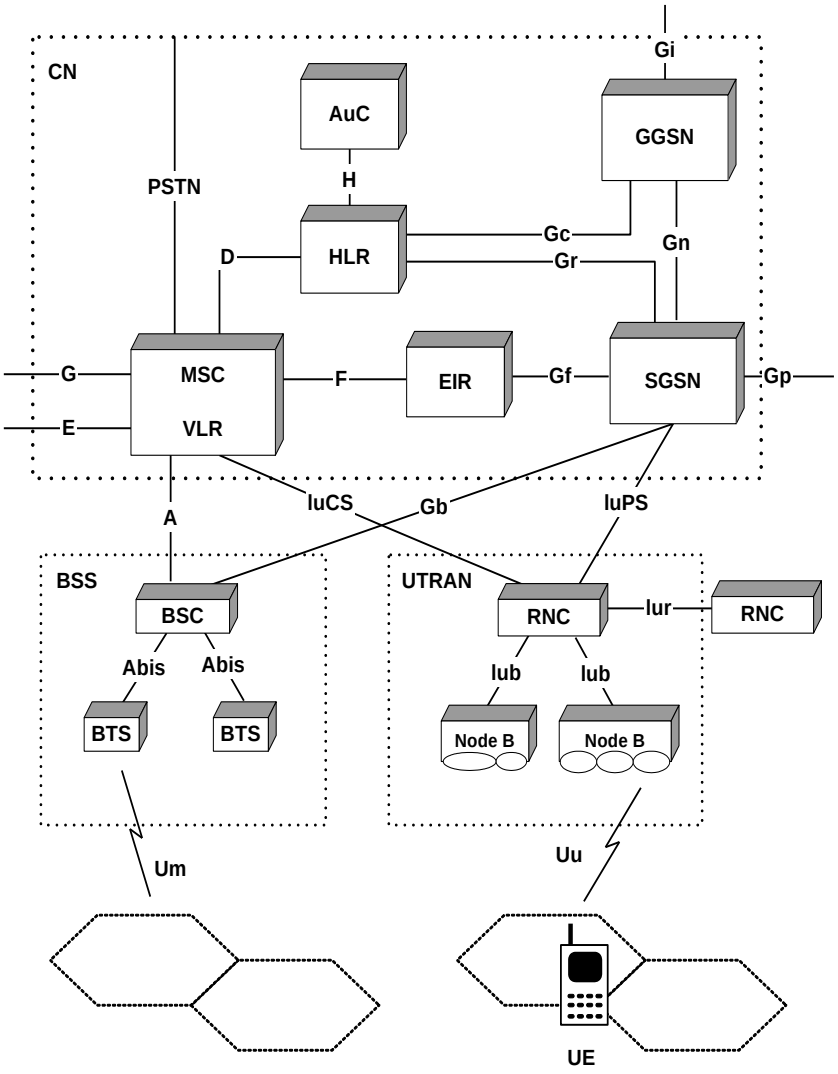
- Το UMTS είναι αντιπρόσωπος των δικτύων τρίτης γενιάς (3G)
- Οι χρήστες έχουν πρόσβαση σε υπηρεσίες υψηλών απαιτήσεων, ανεξαρτήτως θέσης
- Τα κινητά δίκτυα αποτελούν προέκταση του ενσύρματου δικτύου
- Ολοκληρώνει το Διαδίκτυο με τα κινητά δίκτυα
- Το UMTS έχει τυποποιηθεί σε διάφορες εκδόσεις
  - Release 1999, Release 4, Release 5, Release 6…….
- Είναι συμβατό με το δίκτυο GSM/GPRS

Universal Mobile Telecommunication System (UMTS) /2

- Αυξημένους ρυθμούς μετάδοσης και ταυτόχρονη υποστήριξη μεγαλύτερου όγκου δεδομένων και φωνής.
- Θεωρητικά προσφέρει ρυθμούς μετάδοσης δεδομένων έως και 384 kbit/s
  - σε περιπτώσεις όπου παρατηρείται αυξημένη κινητικότητα του χρήστη (vehicular).
- Αντίθετα, όταν ο χρήστης είναι πεζός ή παραμένει ακίνητος, οι ρυθμοί μετάδοσης αυξάνουν κατά πολύ πλησιάζοντας την θεωρητική τιμή των 2 Mbit/s

UMTS /1

- UMTS (Rel. 99)
  - Δίκτυο κορμού (Core Network-CN)
  - Δίκτυο Πρόσβασης (Access Network-AN)
  - Συσκευή Χρήστη (Users' equipment –UE)
- Διαφορά με GSM/GPRS
  - UTRAN (2 Mbps)
  - Wideband Code Division Multiple Access (WCDMA)



UMTS /2

- Ένα δίκτυο κορμού CN μπορεί να λειτουργεί ως
  - οικείο δίκτυο (Home Network)
  - ή ως δίκτυο εξυπηρέτησης (Serving Network, SN)
  - Το SN έχει συνάψει συμφωνία (roaming agreement) με το οικείο δίκτυο του συνδρομητή
    - με σκοπό να εξυπηρετεί χρήστη όταν κινείται (roaming) στην περιοχή που καλύπτει.
    - υπό την προϋπόθεση ότι στην ίδια περιοχή δεν παρέχει επαρκή ή συνήθως καθόλου κάλυψη το οικείο δίκτυο του συνδρομητή.

Ασφάλεια στο UMTS /1

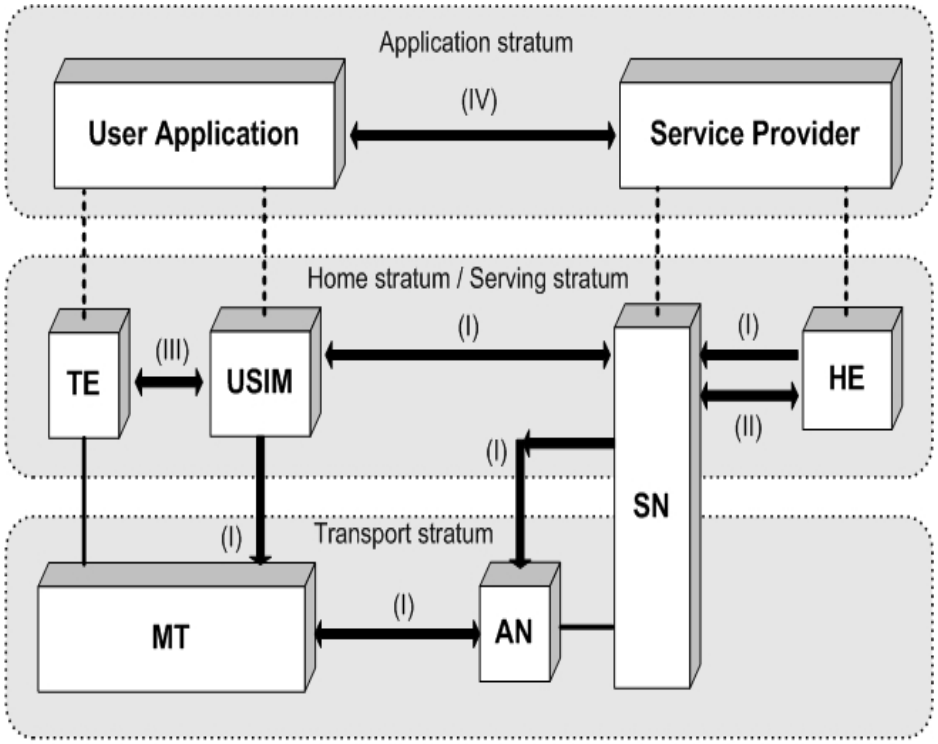
- Η ασφάλεια στο UMTS βασίζεται σε αυτή του GSM/GPRS (αναβαθμίσεις – βελτιώσεις)
- Οι βασικοί μηχανισμοί ασφάλειας διατηρούνται όπως: έλεγχος αυθεντικότητας, κρυπτογράφηση, προστασία της ταυτότητας
- Βασικός στόχος είναι η προστασία:
  - των πληροφοριών που παράγονται ή είναι σχετικές με τον χρήστη
  - των πόρων και των υπηρεσιών του συστήματος

Ασφάλεια στο UMTS /2

- Τα επίπεδα προστασίας και ασφάλειας του UMTS είναι ανώτερα αυτών των σύγχρονων σταθερών & κινητών δικτύων
- Επαρκής τυποποίηση ➔ διαλειτουργικότητα – περιαγωγή
- Οι μηχανισμοί ασφάλειας μπορούν επεκταθούν και να ενισχυθούν ώστε να αντιμετωπίσουν
  - Τις αυξανόμενες απαιτήσεις των νέων υπηρεσιών !!!
  - Τις νέες απειλές !!!

Αρχιτεκτονική ασφάλειας στο UMTS

- Ασφάλεια στο δίκτυο πρόσβασης (I)
- Ασφάλεια στο σταθερό δίκτυο (II)
- Ασφάλεια χρήστη (III)
- Ασφάλεια εφαρμογής (IV)
- Παρουσίαση και διαμόρφωση των μηχανισμών ασφάλειας (V)



Ασφάλεια στο δίκτυο πρόσβασης /1

- Ένα σύνολο μηχανισμών ασφάλειας οι οποίοι
  - Παρέχουν στους χρήστες ασφαλή πρόσβαση στις υπηρεσίες 3G
  - Προστατεύουν την ασύρματη διεπαφή από διάφορες επιθέσεις
- Περιλαμβάνουν
  - Εμπιστευτικότητα της ταυτότητας του χρήστη
  - Έλεγχος της αυθεντικότητας της ταυτότητας του χρήστη και μηχανισμό ανταλλαγής κλειδιών
  - Διατήρηση της εμπιστευτικότητας των δεδομένων
  - Προστασία της ακεραιότητας των μηνυμάτων σηματοδοσίας

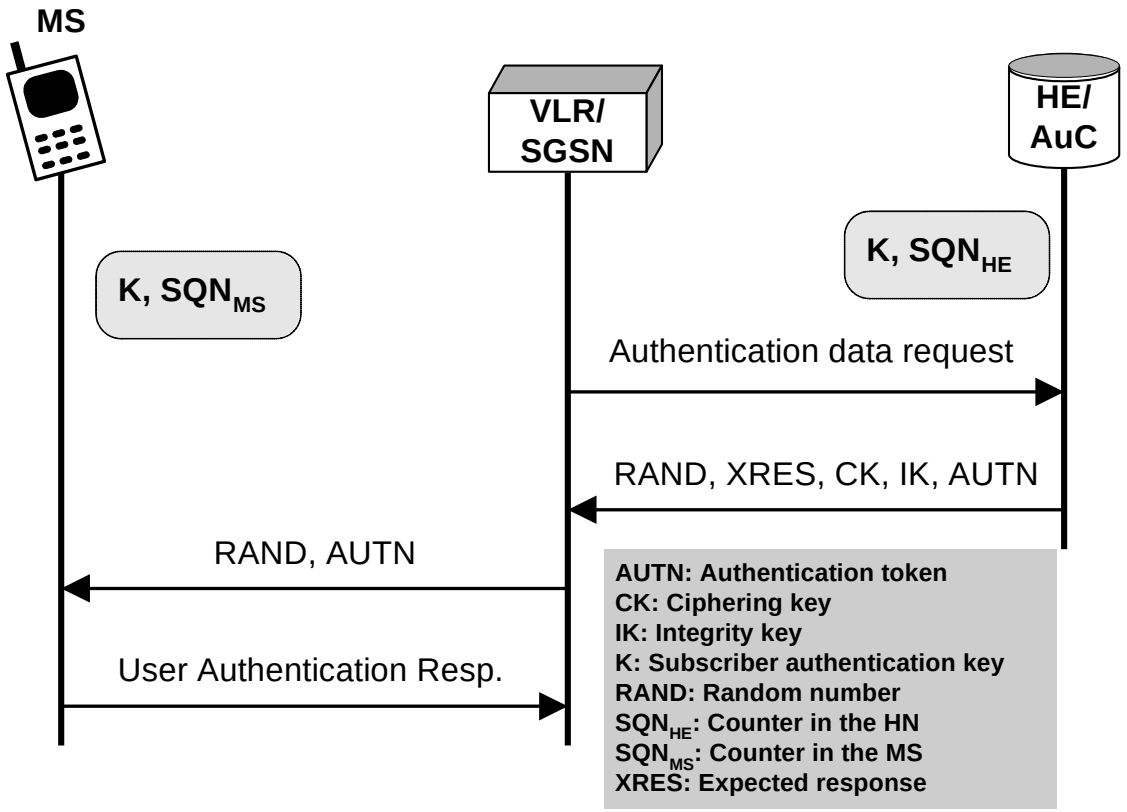
Ασφάλεια στο δίκτυο πρόσβασης /2

- Εμπιστευτικότητα της ταυτότητας του χρήστη
  - International Mobile Subscriber Identity (IMSI)
  - Temporary Mobile Subscriber Identity (TMSI)
    - TMSI έχει μόνο τοπική σημασία
    - Ο συσχετισμός μεταξύ TMSI και IMSI αποθηκεύεται στους κόμβους VLR και SGSN
    - Το TMSI πρέπει να αλλάζει "συχνά"
  - Όταν ο χρήστης κινείται, γίνεται ενημέρωση της συσχέτισης μεταξύ TMSI και IMSI
  - Όταν δεν είναι δυνατή αυτή η συσχέτιση, τότε ο χρήστης μεταφέρει το IMSI πάνω από ασύρματο δίκτυο.

Ασφάλεια στο δίκτυο πρόσβασης /3

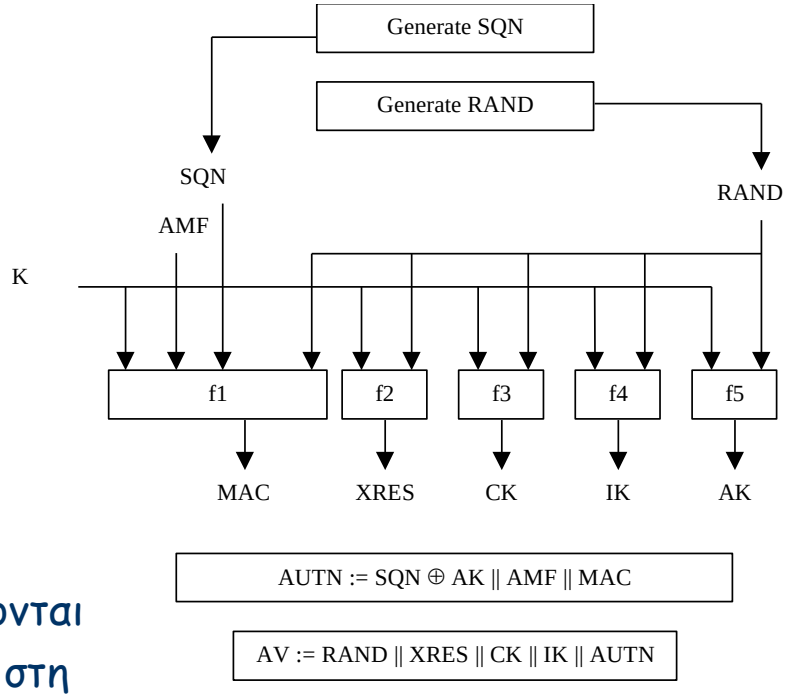
- Αμοιβαίος έλεγχος για την αυθεντικότητα του χρήστη και του δικτύου και ανταλλαγή κλειδιών

- SQN_{HE} μετρητής για τον χρήστη
- SQN_{MS} δείχνει τον μεγαλύτερο αριθμό ακολουθίας που έχει δεχθεί η USIM
- Authentication Vector



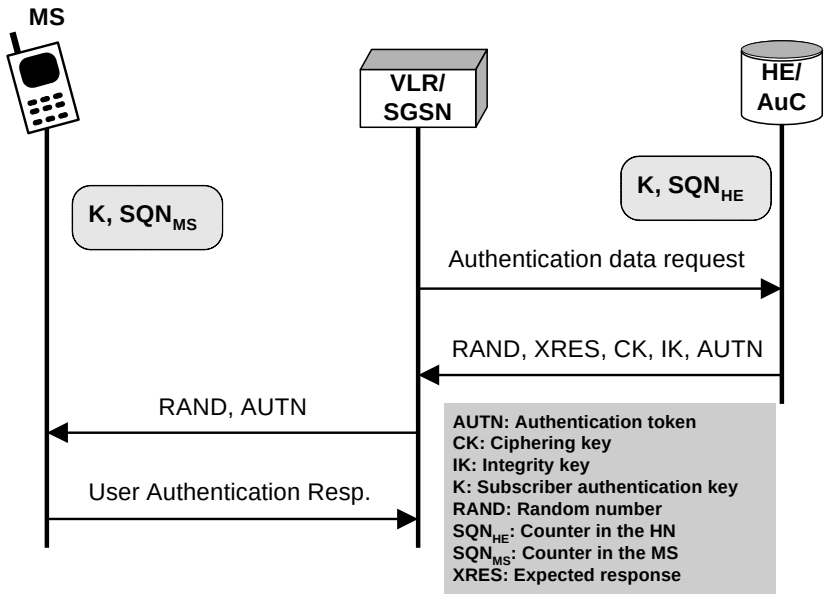
Ασφάλεια στο δίκτυο πρόσβασης /4

- Παραγωγή Authentication Vector (AV)
- MAC = f1k (SQN || RAND || AMF)
- XRES = f2k (RAND)
- Cipher Key CK = f3k (RAND)
- Integrity Key IK = f4k (RAND)
- Anonymity key AK = f5k (RAND)
- AUTN : κουπόνι αυθεντικότητας
- f1, f2 : authentication functions
- F3, f4, f5 : key generation functions
- F1-f5, μονόδρομες συναρτήσεις, βασίζονται στον ίδιο αλγόριθμο, είναι υλοποιημένα στη USIM κάρτα και στο AuC, επιλέγονται από τον πάροχο.



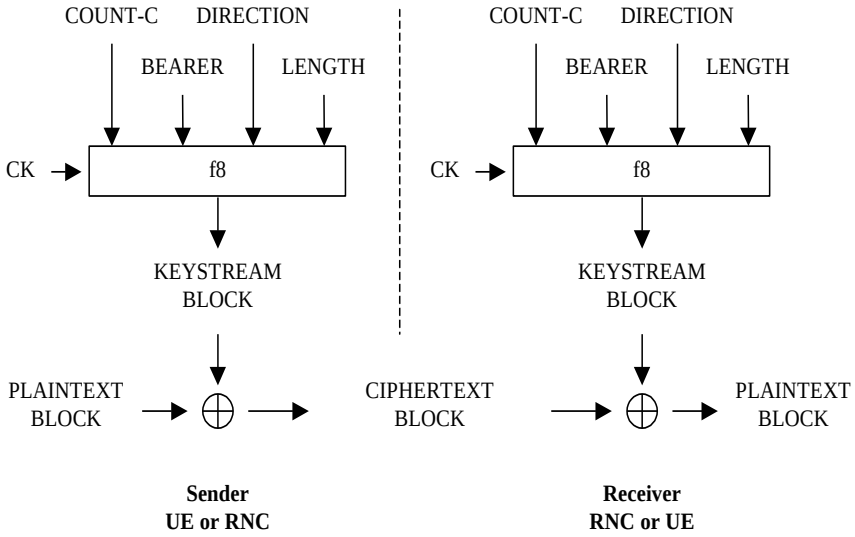
Ασφάλεια στο δίκτυο πρόσβασης /5

- Το δίκτυο στέλνει στη USIM : RAND, AUTN
- Η USIM υπολογίζει και εξετάζει
  - AK = f5k (RAND)
  - SQN = (SQN ⊕ AK) ⊕ AK, η ποσότητα (SQN ⊕ AK) περιλαμβάνεται στο AUTN
  - XMAC = f1k (SQN || RAND || AMF)
  - Ελέγχει MAC (AUTN) ? XMAC
  - Ελέγχει SQN ? SQN_{MS}
  - CK = f3k (RAND)
  - IK = f4k (RAND



Ασφάλεια στο δίκτυο πρόσβασης /6

- Εμπιστευτικότητα των δεδομένων του χρήστη και της σηματοδοσίας (MS – RNC)
  - f8 συμμετρικός αλγόριθμος (Kasumi)
  - CK 128 bits
  - δεν παρέχεται στο φυσικό επίπεδο



Ασφάλεια στο δίκτυο πρόσβασης /7

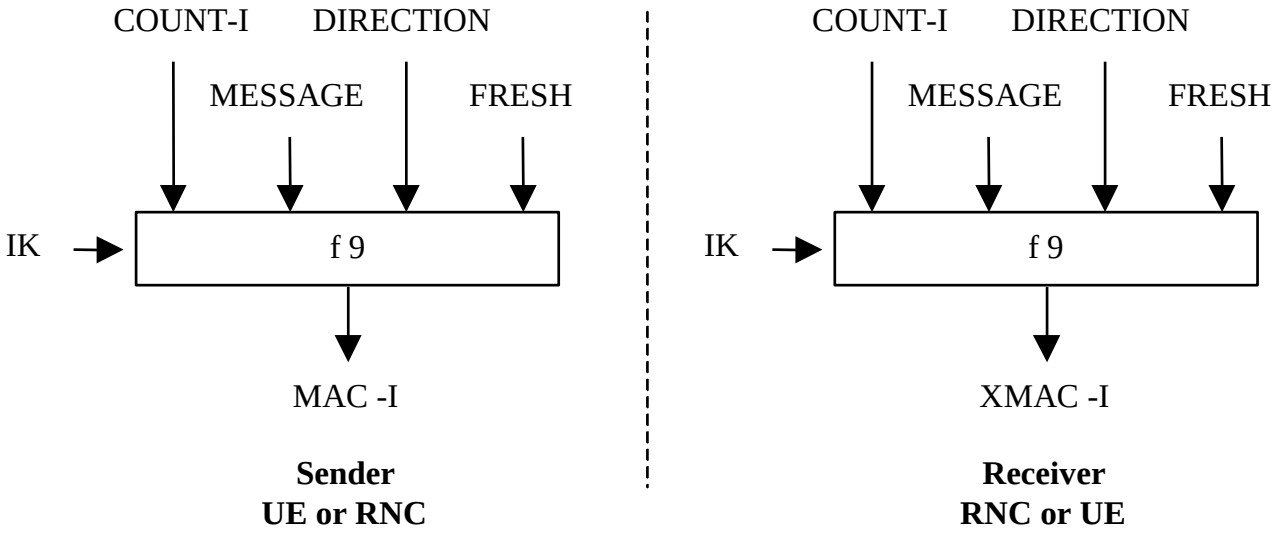
- Ένα ενδιαφέρον σημείο είναι ότι:
  - Η διαδικασία αυθεντικοποίησης δεν είναι πάντα αναγκαία κατά την έναρξη μιας σύνδεσης.
  - Μπορεί να χρησιμοποιηθεί το κλειδί CK που είχε συμφωνηθεί κατά την αμέσως προηγούμενη σύνδεση.
  - Το κλειδί CK, αποθηκεύεται στη USIM,
  - μαζί με αυτό και μια άλλη παράμετρο, η οποία καλείται START.

Ασφάλεια στο δίκτυο πρόσβασης /8

- Για κάθε νέα σύνδεση, η παράμετρος START αυξάνεται κατά 2
- Στη USIM αποθηκεύεται ακόμα μια παράμετρος που ονομάζεται **THRESHOLD**
  - χρησιμοποιείται προκειμένου να περιορίσει τη διάρκεια ζωής των κλειδιών CK και IK.
  - κάθε φορά που η παράμετρος START φτάνει την τιμή της THRESHOLD,
  - η διαδικασία δημιουργίας νέων κλειδιών εκκινείται από το UE.

Ασφάλεια στο δίκτυο πρόσβασης /9

- Προστασία της ακεραιότητας των μηνυμάτων σηματοδοσίας (MS – RNC)
  - Διασφαλίζει την ακεραιότητα και την προέλευση των μηνυμάτων
  - f9 συνάρτηση κατακερματισμού (Kasumi)
  - MAC 32 bits

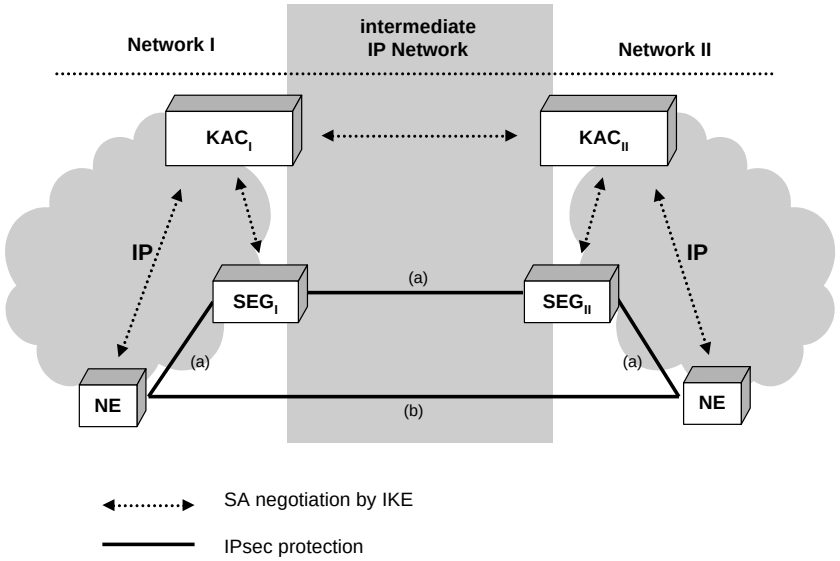


Ασφάλεια στο σταθερό δίκτυο /1

- Μηχανισμοί ασφάλειας στο σταθερό δίκτυο – Network domain security – NDS
  - Προστατεύουν τη σηματοδοσία (control plane)
    - Στο σταθερό δίκτυο κορμού
    - Σε ολόκληρο το ενσύρματο δίκτυο
  - Πρωτόκολλα
    - Mobile Application Part (Signaling System 7 – SS7)
    - GPRS Tunneling Protocol – GTP (IP based)
    - Συνδυασμός των παραπάνω

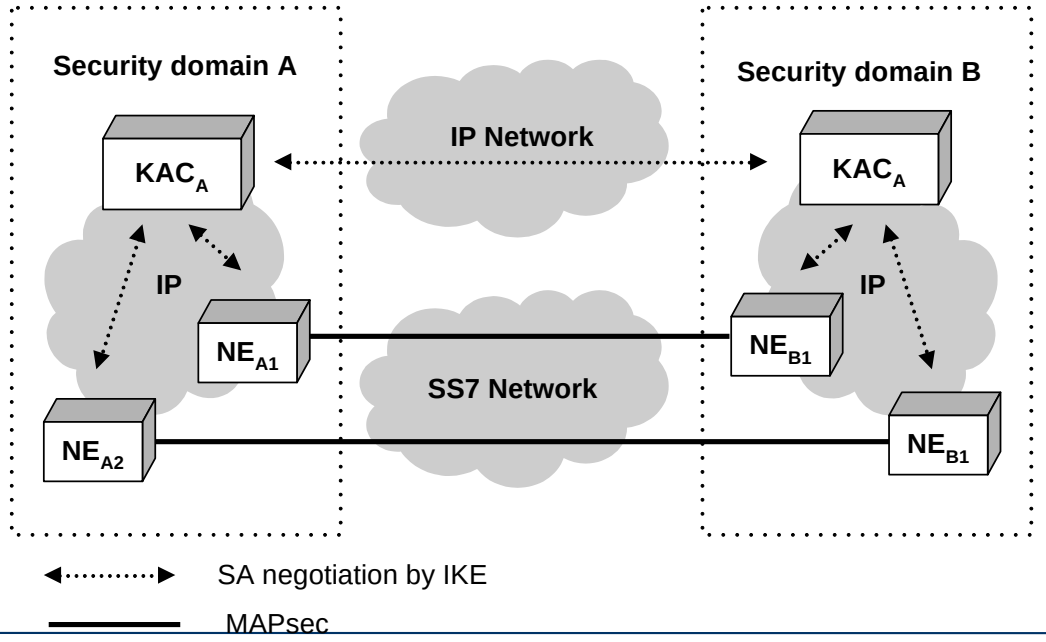
Ασφάλεια στο σταθερό δίκτυο /2

- Πρωτόκολλα που βασίζονται στο IP (GTP)
  - Ασφάλεια σε επίπεδο δικτύου (IPsec)
  - Προορίζεται για τις επόμενες εκδόσεις του UMTS
  - Security domains
  - Security Gateways (SEG)
  - Key Administration Center (KAC)
  - IKE, IPsec
  - End-to-end (b)
  - Hop-by-hop (a)
  - IPsec: Transport or tunnel mode
  - Pre-shared key
  - PKI



Ασφάλεια στο σταθερό δίκτυο /3

- Πρωτόκολλα που βασίζονται στο SS7 ή SS7 & IP
  - Ασφάλεια σε επίπεδο εφαρμογής
  - Προορίζεται για τις επόμενες εκδόσεις του UMTS
  - MAPsec: εμπιστευτικότητα, ακεραιότητα, έλεγχο προέλευσης δεδομένων, προστασία από επιθέσεις επανάληψης.
  - IKE
  - Domain of Interpretation



Ασφάλεια χρήστη

- Διασφαλίζει την πρόσβαση στον κινητό σταθμό
  - Βασίζεται στην κάρτα USIM (User Service Identity Module)
    - Είναι υπεύθυνη για τη διαδικασία ελέγχου της αυθεντικότητας του χρήστη
    - Περιέχει το IMSI και τα κλειδιά του χρήστη
    - Αντίγραφο του προφίλ του χρήστη
    - Η πρόσβαση στη USIM περιορίζεται σε έναν χρήστη ή σε ένα σύνολο εξουσιοδοτημένων χρηστών
      - Γνώση ενός κωδικού (PIN)

Ασφάλεια εφαρμογής

- Ασφαλείς συναλλαγές μεταξύ των MSs και δικτύου εξυπηρέτησης ή του παροχέα υπηρεσιών
  - Απαραίτητο γιατί δεν υπάρχει από άκρο-σε-άκρο ασφάλεια σε χαμηλότερο επίπεδο
  - USIM Application Toolkit ➔ δημιουργεί εφαρμογές που εδρεύουν στη USIM
    - Υποστηρίζει υπηρεσίες ασφάλειας:
      - Αυθεντικοποίηση οντοτήτων & μηνυμάτων
      - Ανίχνευση επαναλήψεων, διασφάλιση ακεραιότητας,
      - Διατήρηση εμπιστευτικότητας, απόδειξη παραλαβής

Παρουσίαση και διαμόρφωση των μηχανισμών ασφάλειας /1

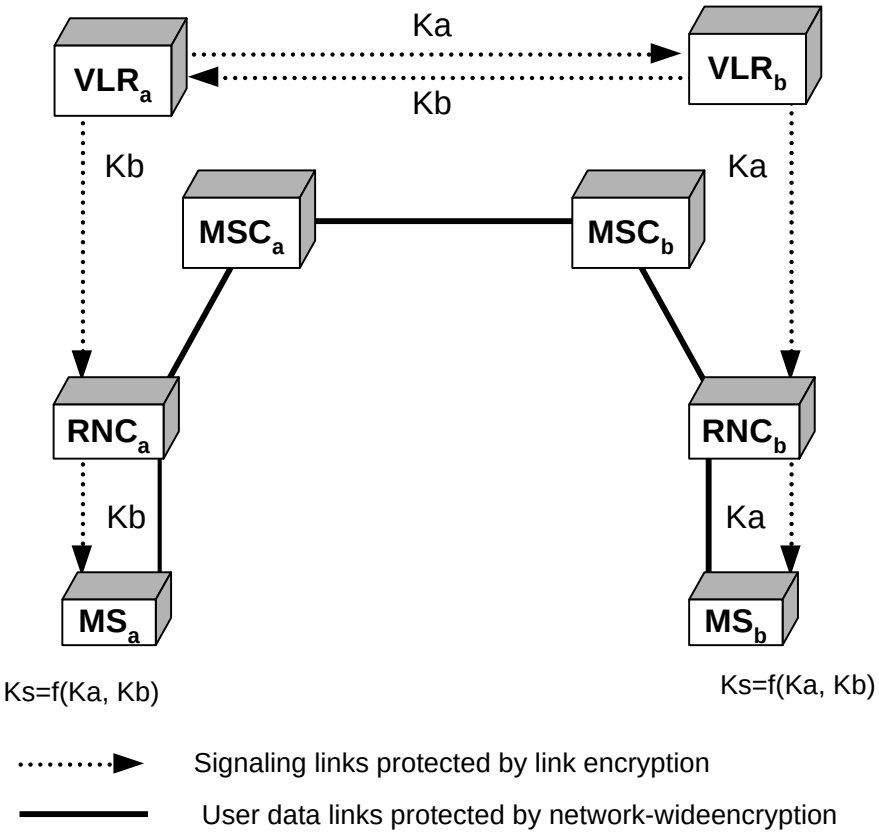
- Παρουσίαση
  - Τα μέτρα ασφάλειας του δικτύου είναι διαφανή ως προς τους χρήστες
  - Οι χρήστες έχουν τη δυνατότητα να γνωρίζουν τα επιμέρους χαρακτηριστικά τους
    - Την ένδειξη παρουσίας κρυπτογράφησης στο δίκτυο
    - Την ένδειξη κρυπτογράφησης εύρους δικτύου
    - Την ένδειξη του επιπέδου ασφάλειας που υποστηρίζεται (π.χ., όταν ένας χρήστης κινείται από ένα δίκτυο 3G προς ένα 2G).

Παρουσίαση και διαμόρφωση των μηχανισμών ασφάλειας /2

- Διαμόρφωση
  - Επιτρέπει στο MS και στο δίκτυο να συνδυάσουν
    - Την παροχή κάποιων υπηρεσιών ⇔ την ενεργοποίηση συγκεκριμένων μηχανισμών ασφάλειας
    - Επιλογές διαμόρφωσης
      - την ενεργοποίηση/απενεργοποίηση του ελέγχου της αυθεντικότητας του χρήστη
      - την αποδοχή/απόρριψη των εισερχόμενων μη-κρυπτογραφημένων κλήσεων (non-ciphered)
      - την εγκατάσταση ή όχι μη-κρυπτογραφημένων κλήσεων
      - την αποδοχή/απόρριψη της χρήσης ορισμένων αλγορίθμων κρυπτογράφησης.

Αρχιτεκτονική ασφάλειας στο UMTS

- Κρυπτογράφηση εύρους δικτύου
  - Δεν έχει προ-τυποποιηθεί ακόμα

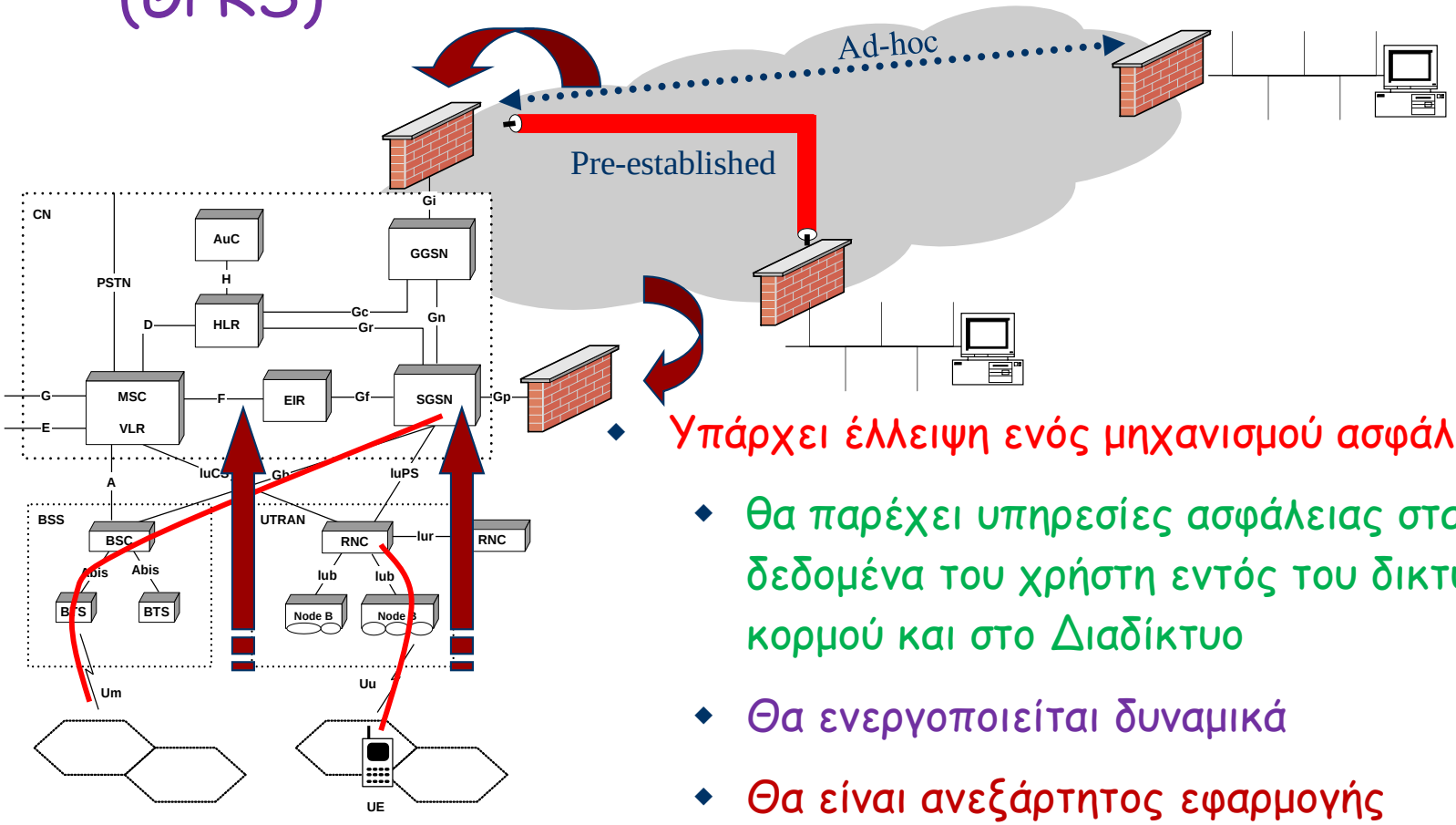


Συμπληρωματικά μέτρα ασφάλειας στο UMTS

- Αναχώματα ασφάλειας (firewalls)
  - Εφαρμογή πολιτικής ασφάλειας
- Προ-εγκατεστημένα VPNs που βασίζονται στο πρωτόκολλο IPsec
  - Στατικά
- Ασφάλεια σε επίπεδο εφαρμογής
  - SSL και WTLS (ασφάλεια στο WAP)
  - SPECSA και Tiny SESAME
  - Συσχέτιση με την εφαρμογή

Αδυναμίες ασφάλειας /1

- Ασφάλεια σε επίπεδο δεδομένων του χρήστη (GPRS)



- Υπάρχει έλλειψη ενός μηχανισμού ασφάλειας
  - Θα παρέχει υπηρεσίες ασφάλειας στα δεδομένα του χρήστη εντός του δικτύου κορμού και στο Διαδίκτυο
  - Θα ενεργοποιείται δυναμικά
  - Θα είναι ανεξάρτητος εφαρμογής

Αδυναμίες ασφάλειας /2

- Αρκετά γνωστά προβλήματα και αδυναμίες του μηχανισμού αυθεντικοποίησης του GSM φαίνεται ότι έχουν λυθεί ή επαρκώς καλυφθεί στον αντίστοιχο του UMTS.

- Παρόλα αυτά, υπάρχουν ακόμη ορισμένα κενά ασφαλείας ή αδυναμίες, τις οποίες οι επιτιθέμενοι μπορούν να εκμεταλλευτούν.

Αδυναμίες ασφάλειας /3

- Επιτιθέμενοι που εφαρμόζουν παθητικές (passive) ή ενεργητικές (active) μεθόδους,
  - μπορούν να υποκλέψουν διανύσματα (vectors) αυθεντικοποίησης
    - είτε από τα SGSN & HSS είτε από το δίαυλο επικοινωνίας μεταξύ αυτών.
  - απαιτείται ιδιαίτερη προσοχή όταν ένας συνδρομητής βρίσκεται σε κατάσταση περιαγωγής-roaming.
    - Το οικείο δίκτυο είναι υποχρεωμένο να αποστείλει στο δίκτυο εξυπηρέτησης τα διανύσματα αυθεντικοποίησης
    - Έτσι το SN μπορεί να αυθεντικοποιήσει το συνδρομητή.

Αδυναμίες ασφάλειας /4

- Τα διανύσματα αυθεντικοποίησης μεταφέρονται μεταξύ των διαφορετικών δικτύων των παρόχων
  - οι οποίοι μπορεί να εφαρμόζουν διάφορες πολιτικές ασφαλείας
  - είναι πολύ πιθανό να υποκλαπούν ή να καταστραφούν.
- Οι χρήστες πρέπει να εμπιστεύονται το δίκτυο εξυπηρέτησης
  - Καθώς και τις πολιτικές ασφάλειας που αυτό εφαρμόζει.

Αδυναμίες ασφάλειας / 5

- Υπάχουν περιπτώσεις που το σύστημα επιτρέπει την εκπομπή του IMSI του χρήστη σε μορφή καθαρού κειμένου (clear-text)
  1. Όταν ο συνδρομητής εγγράφεται για πρώτη φορά στο δίκτυο
  2. Μετά από μεγάλο διάστημα κατά το οποίο διατηρούσε τη συσκευή του εκτός λειτουργίας
  3. Όταν το δίκτυο δεν μπορεί να ανακτήσει το IMSI του συνδρομητή. Π.χ., σε περιπτώσεις μεταβίβασης κλήσης ή συνεδρίας (session) από κυψέλη σε κυψέλη ή από δίκτυο σε δίκτυο (handover)
  4. Όταν η βάση δεδομένων ενός SGSN παρουσιάζει βλάβη
- Υπάρχουν τοποθεσίες ή σημεία στα οποία πολλά IMSIs εκπέμπονται συνεχώς.
  - σημεία όπου οι χρήστες ανοίγουν τα κινητά τους μετά την πτήση ή γενικότερα το ταξίδι τους.

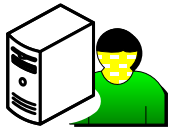
Αδυναμίες ασφάλειας /6

- Η διαδικασία αυτή είναι ανοικτή σε παθητικού τύπου επιθέσεις,
  - ο επιτιθέμενος περιμένει για πιθανές εκπομπές απροστάτευτων IMSI
  - ή σε επιθέσεις τύπου Man-in-the-Middle (MITM).
- Η αποκάλυψη του IMSI αποτελεί
  - παραβίαση της εμπιστευτικότητας της ταυτότητας του χρήστη (identity confidentiality)
  - παραβίαση της θέσης που αυτός κινείται (location privacy).
- Η γνώση του IMSI μπορεί να επιτρέψει την πλαστογράφηση της ταυτότητας του χρήστη.

Αδυναμίες ασφάλειας /7

- Ο μηχανισμός αυθεντικοποίησης του UMTS δεν προσφέρει προστασία από ένα ενεργό επιτιθέμενο, ο οποίος μπορεί να προσποιηθεί (masquerade) το δίκτυο εξυπηρέτησης (false base station - RNC attack) με αποτέλεσμα να καταφέρει εύκολα να αποκτήσει το IMSI του χρήστη θύματος.

MS (SIM)
IMSI / (P)-TMSI Ki



Επιτιθέμενος

TMSI →

← Sorry, Unknown TMSI or VLR/SGSN not reachable

← Identity Request

IMSI [acquired by the attacker] →

Αδυναμίες ασφάλειας /8

- Το μήκος των κλειδιών και οι αλγόριθμοι κρυπτογράφησης / αποκρυπτογράφησης είναι σταθερά (fixed).

- Οι μηχανισμοί ασφάλειας του UMTS είναι δύσκαμπτοι (inflexible) → κενά ασφάλειας

- Αν ανακαλυφθεί μια ευπάθεια (vulnerability) σε κάποιον αλγόριθμο ή διαδικασία, όπως στην περίπτωση του αλγορίθμου GSM A5/1, τότε δεν μπορει εύκολα να αντικατασταθεί.

Αδυναμίες ασφάλειας /9

- Μια από τις βελτιώσεις ασφαλείας στο UMTS σε σχέση με το GSM είναι η δυνατότητας προστασίας της ακεραιότητας.
  - Όμως, η προστασία της ακεραιότητας είναι εγγυημένη μόνο για τη σηματοδοσία και μόνο μεταξύ UE και RNC.
- Στα δεδομένα των χρηστών δεν προσαρτάται Message Authentication Code (MAC)
  - για λόγους απόδοσης (performance)
  - γι' αυτό το λόγο είναι τρωτά σε παραποιήσεις (manipulation).

Προτάσεις ασφάλειας

- Χρήση σχημάτων για δυναμική ανάπτυξη VPNs που βασίζονται στο πρωτόκολλο IPsec
  - Από άκρο σε άκρο (end-to-end)
  - Network assisted
- Χρήση δύο επιπλέον προσωρινών ταυτοτήτων
  - $TMSI_{SN}$ και $TMSI_{HE}$
- Επέκταση των μηχανισμών ασφάλειας για το σταθερό δίκτυο στην πρώτη έκδοση του UMTS (Rel 1999)
- Δυναμικοί μηχανισμοί ασφάλειας, ικανότητα για ενσωμάτωση νέων στοιχείων (modules) ασφαλείας σε πραγματικό χρόνο ανάλογα με τις συνθήκες (on-demand)

Σύστημα νομίμων συνακροάσεων (Lawful Interception) /1

- Η νομοθεσία των περισσοτέρων χωρών υπαγορεύει ότι οι αρχές (authorities) θα έχουν τη δυνατότητα πρόσβασης
  - σε ευαίσθητες πληροφορίες και δεδομένα των συνδρομητών
  - π.χ., οι αστυνομικές αρχές μετά από εισαγγελική άδεια ή εντολή θα πρέπει να είναι ικανές σε συνεργασία με τον πάροχο των τηλεπικοινωνιακών υπηρεσιών να ακούν συνομιλίες υπόπτων για εγκληματικές πράξεις ή να παρακολουθούν τις κινήσεις τους.
- Τα στοιχεία αυτά μπορούν να χρησιμοποιούνται ως αποδείξεις στις δικαστικές αίθουσες.

Σύστημα νομίμων συνακροάσεων (Lawful Interception) /2

- Στο σύστημα GSM, η δυνατότητα νομίμων συνακροάσεων με τη μορφή αντίστοιχου υλισμικού προστέθηκε εκ των υστέρων.
- Αντιθέτως, στο UMTS η συγκεκριμένη δυνατότητα – υπηρεσία απασχόλησε τους σχεδιαστές του συστήματος εξ αρχής
  - αποτέλεσμα να θεσπιστούν λεπτομερείς προδιαγραφές για κάθε χαρακτηριστικό της και κάθε σημείο διεπαφής της με το υπόλοιπο σύστημα.
- Έτσι έχουν οριστεί συγκεκριμένες αρχιτεκτονικές για το σύστημα νομίμων συνακροάσεων σε διάφορα σημεία του δικτύου.

Σύστημα νομίμων συνακροάσεων (Lawful Interception) /3

- Λαμβάνεται υπόψη κάθε νέα υπηρεσία ή δυνατότητα που προστίθεται στο σύστημα
- Σε περίπτωση που τα δεδομένα συνακρόασης (intercept data) είναι πραγματικού χρόνου παρακολουθείται
  - το περιεχόμενο μιας συνομιλίας ή το κείμενο ενός μηνύματος SMS
- Πληροφορίες δικτύου
  - η θέση που ο στόχος κινείται, ο χρόνος ενεργοποίησης ή απενεργοποίησης από το στόχο ενός PDP context (GPRS), κ.ά.
- Ο στόχος παρακολούθησης μπορεί να προσδιορίζεται με βάση το IMSI ή άλλη ταυτότητα (NAI, IMEI).