ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Σχεδίαση και Ανάπτυξη Υπηρεσιών Υποδομής Δημόσιων Κλειδιών στα Δίκτυα Κινητών Επικοινωνιών Τρίτης και Ύστερων Γενεών

Διδακτορική διατριβή

Καμπουράκη Γεώργιου

Σάμος, Νοέμβριος 2004

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Συμβουλευτική Επιτροπή:

Πρόεδρος:

Στέφανος Γκρίτζαλης
Αναπληρωτής Καθηγητής
Πανεπιστημίου Αιγαίου

Μέλη:

Σωκράτης Κ. Κάτσικας
Καθηγητής
Πανεπιστημίου Αιγαίου

Άγγελος Ρούσκας
Επίκουρος Καθηγητής
Πανεπιστημίου Αιγαίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ
ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΑΤΡΙΒΗ

Για την απόκτηση Διδακτορικού Διπλώματος
του Τμήματος Μηχανικών Πληροφοριακών και
Επικοινωνιακών Συστημάτων

Καμπουράκη Γεώργιου

Σχεδίαση και Ανάπτυξη Υπηρεσιών Υποδομής Δημόσιων Κλειδιών στα Δίκτυα Κινητών Επικοινωνιών Τρίτης και Ύστερων Γενεών

Εξεταστική Επιτροπή:

Πρόεδρος:

Στέφανος Γκρίτζαλης
Αναπληρωτής Καθηγητής Πανεπιστημίου Αιγαίου

Μέλη:

Σωκράτης Κ. Κάτσικας
Καθηγητής Πανεπιστημίου Αιγαίου

Νικόλαος Αλεξανδρής
Καθηγητής Πανεπιστημίου Πειραιώς

Βασίλειος Χρυσικόπουλος
Καθηγητής Ιονίου Πανεπιστημίου

Νικήτας Νικητάκος
Αναπληρωτής Καθηγητής Πανεπιστημίου Αιγαίου

Άγγελος Ρούσκας
Επίκουρος Καθηγητής Πανεπιστημίου Αιγαίου

Κωνσταντίνος Λαμπρινουδάκης
Λέκτορας Πανεπιστημίου Αιγαίου

στην οικογένειά μου …

Come gather 'round people
Wherever you roam
And admit that the waters
Around you have grown
And accept it that soon
You'll be drenched to the bone.
If your time to you
Is worth savin'
Then you better start swimmin'
Or you'll sink like a stone
For the times they are a-changin'

(Bob Dylan – The times they are A-Changin')

Πρόλογος και ευχαριστίες

Η παρούσα διατριβή είναι το προϊόν ερευνητικής εργασίας που πραγματοποιήθηκε στο Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου στη Σάμο. Την προσπάθεια αυτή συνέδραμαν αρκετοί άνθρωποι τους οποίους θα ήθελα να ευχαριστήσω.

Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω την τριμελή επιτροπή μου και ιδιαίτερα τον αναπληρωτή καθηγητή Στέφανο Γκρίτζαλη και τον Επίκουρο καθηγητή Άγγελο Ρούσκα για την αδιάλειπτη και ουσιαστική υποστήριξή τους και για το σημαντικό χρόνο και κόπο που κατέβαλαν για το σκοπό αυτό. Η βοήθεια, η συμπαράσταση και η ειλικρινής φιλία τους υπήρξε αμέριστη και απολύτως καθοριστική για την ολοκλήρωση αυτής της προσπάθειας.

Επίσης θα ήθελα να ευχαριστήσω το μεταπτυχιακό φοιτητή Γενειατάκη Δημήτριο για την ουσιαστική βοήθεια που πρόσφερε σε διαφορετικά στάδια της παρούσας διατριβής.

Ευχαριστώ επίσης τους μεταπτυχιακούς φοιτητές Σάρκο Γεώργιο, Καρόπουλο Γεώργιο, Ευδωρίδη Θεόδωρο και Λίζο Κωνσταντίνο για τη συμβολή τους σε ορισμένα ζητήματα της ερευνητικής αυτής προσπάθειας.

Τέλος, θα ήθελα να ευχαριστήσω τους δασκάλους μου και φιλολόγους Θεόδωρο Σαρρηγιάννη και Κάτια Ζαχαρίου για τις διορθώσεις και τις παρατηρήσεις τους στο τελικό κείμενο της διατριβής.

Πίνακας Περιεχομένων

Ακρωνύμια και Βραχυγραφίες

1G	1st Generation	Πρώτη γενιά κινητών επικοινωνιών
2G	2nd Generation	Δεύτερη γενιά κινητών επικοινωνιών
3G	3rd Generation	Τρίτη γενιά κινητών επικοινωνιών
3GPP	3rd Generation Partnership Project	Οργανισμός προτυποποίησης συστημάτων 3G
4G	4th Generation	Τέταρτη γενιά κινητών επικοινωνιών
AA	Attribute Authority	Αρχή πιστοποίησης Ιδιοτήτων
AAA	Authentication Authorization Accounting	Αυθεντικοποίηση, Εξουσιοδότηση, Λογιστική καταγραφή
AC	Attribute Certificate	Πιστοποιητικό Ιδιοτήτων
AKA	Authentication and Key Agreement	Διαδικασία αυθεντικοποίησης και συμφωνίας κλειδιού
AP	Access Point	Σημείο πρόσβασης σε WLAN
AuC	Authentication Centre	Κέντρο αυθεντικοποίησης συνδρομητών
B3G	Beyond-3G	Δίκτυα μεταγενέστερα των 3G δικτύων
CA	Certification Authority	Αρχή πιστοποίησης
CDMA	Code Division Multiple Access	Τεχνική μετάδοσης με πολύπλεξη κώδικα
CGW	Certificate provisioning Gateway	Πύλη παροχής υπηρεσιών ψηφιακών πιστοποιητικών
CR	Certificates Repository	Αποθήκη πιστοποιητικών
CRL	Certificate Revocation List	Λίστα καταργημένων πιστοποιητικών
CSCF	Call State Control Function	SIP εξυπηρέτης στην 3GPP αρχιτεκτονική
CSP	Certification Service Provider	Πάροχος υπηρεσιών πιστοποίησης
DDoS	Distributed DoS	Κατανεμημένη επίθεση DoS
DHCP	Dynamic Host Configuration Protocol	Πρωτόκολλο αυτόματης απόδοσης διεύθυνσης IP και άλλων συναφών υπηρεσιών
DN	Distinguished Name	Διακεκριμένο όνομα
DNS	Domain Name Server	Εξυπηρέτης επίλυσης ονομάτων τομέων
DoS	Denial of Service	Επίθεση παρακώλυσης της διαθεσιμότητας των υπηρεσιών
EAP	Extensible Authentication Protocol	Πρωτόκολλο 2ου επιπέδου
ESP	Encapsulating Security Payload	Μηχανισμός του πρωτοκόλλου IPsec
FQDN	Fully Qualified Domain Name	Πλήρες όνομα τομέα δικτύου
GGSN	Gateway GPRS Support Node	Στοιχείο αρχιτεκτονικής δικτύων 2.5/3G
GPRS	General Packet Radio Service	Υπηρεσία δεδομένων σε συστήματα GSM/UMTS
GSM	Global System for Mobile Communication	Σύστημα κινητών επικοινωνιών 2G
HiPERLAN	High Performance Radio LAN	Ανταγωνιστικό με το 802.11 πρότυπο ασύρματων δικτύων - Λειτουργεί στις συχνότητες των 5 GHz
HN	Home Network	Δίκτυο που ανήκει (ή έχει εγγραφεί) ο συνδρομητής
HSS	Home Subscriber Server	Στοιχείο αρχιτεκτονικής 3GPP δικτύων μετά την έκδοση 4
ICC	Integrated Circuit Chip	Ενσωματωμένο ολοκληρωμένο κύκλωμα σε έξυπνη κάρτα

IKE	Internet Key Exchange	Υπεύθυνο πρωτόκολλο για την εγκαθίδρυση SAs στη σουίτα IPsec
IMSI	International Mobile Subscriber Identity	Μοναδικός αριθμός αναγνώρισης συνδρομητή
ITSP	Internet Telephony Service Provider	Πάροχος υπηρεσιών διαδικτύου μέσω τηλεφώνου
ITU	International Telecommunications Union	Διεθνή ένωση τηλεπικοινωνιών
J2ME	Java 2 Micro Edition	Java έκδοση του SSL
LDAP	Lightweight Directory Access Protocol	Πρωτόκολλο αποθήκευσης και ανάκλησης πιστοποιητικών και CRLs
MAC	Message Authentication Code	Προστασία ακεραιότητας
MAP	Mobile Application Protocol	Πρωτόκολλο σηματοδοσίας 2G και 3G συστημάτων
MMS	Multimedia Messaging Service	Υπηρεσία αποστολής πολυμεσικών μηνυμάτων
NDS	Network Domain Security	Μηχανισμοί ασφαλείας που ισχύουν σε τομέα δικτύου
MITM	Man in the Middle	Τύπος επίθεσης σε ενσύρματα και ασύρματα δίκτυα.
NE	Network Element	Στοιχείο ή κόμβος ή οντότητα ενός δικτύου
NMT	Nordic Mobile Telephone	Σύστημα κινητών επικοινωνιών 1G
OCSP	Online Certificates Status Protocol	Πρωτόκολλο για ανάκληση ψηφιακών πιστοποιητικών
PAC	Privilege Access Certificate	Ψηφιακά πιστοποιητικά που χρησιμοποιούνται στο SESAME και στα Microsoft Windows 2000
PDC	Personal Digital Cellular	Σύστημα κινητών επικοινωνιών 2G
PDP	Packet Data Protocol	Πρωτόκολλο εγκαθίδρυσης IP συνδέσεων UE–to-GGSN
PEAP	Protected EAP	Πρωτόκολλο προστασίας EAP
PEP	Performance Enhancing Proxy	Οντότητες δικτύων 3G – βελτιώνουν την απόδοση των TCP συνδέσεων
PMI	Privilege Management Infrastructure	Όρος αντίστοιχος του PKI για υποδομές που χρησιμοποιούν αποκλειστικά AAs και ACs
PKC	Public Key Certificate	Πιστοποιητικό δημόσιου κλειδιού
PKI	Public Key Infrastructure	Υποδομή δημόσιου κλειδιού
PLMN	Public Land Mobile Network Operator	Πάροχος υπηρεσιών κινητών επικοινωνιών
PPC	Pocket PC	Υπολογιστής τσέπης
PS	Packet Switched (domain)	Υποσύστημα του UMTS βασισμένο σε IP (GPRS, IM)
P-TMSI	Packet-Temporary Mobile Subscriber Id.	Προσωρινό αναγνωριστικό συνδρομητή
RA	Registration Authority	Αρχή εγγραφής
RANAP	Radio Access Network Application Protocol	Πρωτόκολλο που εκτελείται μεταξύ RNC και SGSN
RBAC	Role-Based Access Control	Μηχανισμός ελέγχου πρόσβασης βασισμένος σε ρόλους
RNC	Radio Network Controller	Στοιχείο 2.5/3G αρχιτεκτονικής δικτύου
RoA	Roaming Agreement	Συμφωνία μεταγωγής μεταξύ διαφορετικών παρόχων
SA	Security Association	Συσχετισμοί ασφαλείας (πρωτόκολλο IKE)
SEG	Security Gateway	Πύλες ασφαλείας σε 3GPP δίκτυα (IP domain)

SGSN	Serving GPRS Support Node	Στοιχείο αρχιτεκτονικής δικτύων 2.5/3G
SIM	Subscriber Identity Module	Στοιχείο αναγνώρισης συνδρομητή (έξυπνη κάρτα)
SIP	Session Initiation Protocol	Πρωτόκολλο Αρχικοποίησης συνόδου (UMTS IM)
SMS	Short Message Service	Υπηρεσία αποστολής Σύντομων μηνυμάτων κειμένου
SN	Serving Network	Δίκτυο εξυπηρέτησης
SS7	Signalling System Number 7	Πρωτόκολλο δικτύων 2G
SSCD	Secure Signature Creation Devices	Έξυπνη κάρτα δημιουργίας ψηφιακών υπογραφών
SSID	Service Set Identifiers	Αναγνωριστικά δικτύων WLAN 802.11
SSL	Secure Sockets Layer	Πρωτόκολλο ασφαλείας κάτω από το επίπεδο εφαρμογής
TDMA	Time Division Multiple Access	Τεχνική μετάδοσης με πολύπλεξη χρόνου
TLS	Transport Layer Security	Εξέλιξη του πρωτοκόλλου SSL
TTLS	Tunneled TLS	Πρωτόκολλο
TTP	Trusted Third Party	Έμπιστη τρίτη οντότητα
UE	User Equipment	Κινητός εξοπλισμός συνδρομητή
UE	User Equipment	Κινητή Συσκευή ή εξοπλισμός τελικού χρήστη
UICC	USIM ICC	Έξυπνη κάρτα - μπορεί να περιέχει πολλές USIM εφαρμογές
UMTS	Universal Mobile Telecommunications System	Σύστημα κινητών επικοινωνιών 3G
USIM	Universal Subscriber Identity Module	Αντίστοιχη της SIM για το UMTS
WAP	Wireless Application Protocol	Πρωτόκολλο για εφαρμογές κινητής τηλεφωνίας
W-CDMA	Wideband CDMA	Παραλλαγή της τεχνικής CDMA
Wi-Fi	Wireless Fidelity	Δίκτυα του τύπου IEEE 802.11
WLAN	Wireless Local Access Network	Ασύρματα τοπικά δίκτυα
WTLS	Wireless Transport Layer Security	Πρωτόκολλο αντίστοιχο του TLS για ασύρματο περιβάλλον

Περίληψη

Τα ζητήματα που αφορούν την ασφάλεια των συστημάτων κινητών επικοινωνιών έχουν συγκεντρώσει το ενδιαφέρον τόσο των επαγγελματιών και επιστημόνων της πληροφορικής όσο και του ευρύτερου κοινού. Η επιστημονική έρευνα στο χώρο αυτό εντείνεται όσο πλησιάζουμε την προοπτική του ενοποιημένου δικτυακού περιβάλλοντος της τέταρτης γενιάς. Σήμερα, η τρίτη γενιά κινητών επικοινωνιών αποτελεί ήδη γεγονός. Παρόλα αυτά, οι εμπλεκόμενοι οργανισμοί προτυποποίησης, στην προσπάθειά τους να πετύχουν το μέγιστο βαθμό συμβατότητας με τα προηγούμενων γενεών ανάλογα συστήματα, φαίνεται να επιλέγουν για υλοποίηση μεθόδους και διαδικασίες ασφαλείας, που περισσότερο ταιριάζουν σε κλειστά και περιορισμένης εμβέλειας δίκτυα.

Όμως, η εισαγωγή του πρωτοκόλλου IP στα κεντρικά δίκτυα των παρόχων αυτών των υπηρεσιών, το ολοένα αυξανόμενο πλήθος των συνδρομητών, οι πολύπλοκες σχέσεις που αναμένεται να αναπτυχθούν μεταξύ των παρόχων, η διασύνδεση των δικτύων αυτών με το Διαδίκτυο (Internet) και το ετερογενές περιβάλλον πρόσβασης, είναι μερικοί από τους λόγους που τα ζητήματα ασφαλείας απαιτείται να αναθεωρηθούν.

Λαμβάνοντας υπόψη τα αναμενόμενα πλεονεκτήματα της εισαγωγής της τεχνολογίας δημόσιου κλειδιού στα συστήματα κινητών επικοινωνιών τρίτης γενιάς, η ερευνητική προσπάθεια που παρουσιάζεται στην παρούσα διατριβή επικεντρώθηκε στα εξής ζητήματα:

1. Μελέτη των τρόπων εισαγωγής και αξιοποίησης της τεχνολογίας υποδομής δημόσιου κλειδιού στα δίκτυα κινητών επικοινωνιών τρίτης και ύστερων γενεών.
2. Σχεδίαση, ανάπτυξη και αξιολόγηση υπηρεσιών που βασίζονται στην τεχνολογία δημόσιου κλειδιού για τα δίκτυα κινητών επικοινωνιών τρίτης και ύστερων γενεών.

Για την αντιμετώπιση του πρώτου ζητήματος αναλύονται διάφορες αρχιτεκτονικές και προτείνονται συγκεκριμένες μέθοδοι με τις οποίες είναι δυνατό να ενισχυθούν οι διαδικασίες ασφαλείας που αφορούν τόσο τα δίκτυα των παρόχων, όσο και τους ίδιους τους συνδρομητές. Για το δεύτερο ζήτημα, η ανάλυσή μας επικεντρώνεται σε θέματα αυθεντικοποίησης και εξουσιοδότησης των συνδρομητών που κινούνται σε υβριδικά ασύρματα περιβάλλοντα πρόσβασης, μέσω της αξιοποίησης γνωστών πρωτοκόλλων και υπηρεσιών που χρησιμοποιούν τεχνολογία δημόσιου κλειδιού.

Η έρευνα που παρουσιάζεται στην παρούσα διατριβή συμβάλλει στη μελέτη και υποβοηθά στην αντιμετώπιση των παραπάνω state-of-the-art ζητημάτων, ενώ παράλληλα αναλύοντας και οριοθετώντας μια βασική ιδέα, δημιουργεί προοπτικές για περαιτέρω ερευνητική δραστηριότητα στον ίδιο ή συναφείς τομείς.

Abstract

Mobile communications systems security issues have gathered the interest of both the professionals and scientists of information technology as well as the wider public. Moreover, the scientific research on this topic is intensified as long as we approach the prospect of unified network environment of fourth generation (4G). Today, the third generation of mobile communications (3G) is already a reality. Nevertheless, the involved standard organizations in their effort to achieve highest degree of compatibility with previous generations' systems, up to now seem to be conservative and select security methods and procedures that are more suitable to closed and limited scope communications networks.

However, the adoption of the IP protocol in the mobile service providers' core networks, the continuously increasing number of subscribers, the complicated trust relationships that are expected to be developed between the providers, the interconnection of networks with the Internet and the heterogeneous access environment, are only some of the reasons that security issues have to be revised.

Taking into consideration the expected advantages that stem from the incorporation of public key technology into 3G communication systems, the research effort that is presented in the current thesis focused in the following subjects:

1. Study ways to integrate and exploit Public Key Infrastructure (PKI) technology into 3G-and-beyond (B3G) communication systems.

2. Design, develop and evaluate specific services which are based on public key technology for B3G communication networks.

Regarding the first issue, various 3G-to-PKI integration architectures are proposed and analyzed in order to strengthen the security procedures concerning both the service providers as well as the subscribers of 3G-and-beyond communication networks.

In the second topic, our analysis is focused on authentication and authorization of subscribers roaming in hybrid wireless access environments, via the exploitation of known protocols and services that utilize public key technology.

The research presented in this thesis studies and proposes solutions for state-of-the-art security issues in B3G communication systems, while at the same time, creates prospects for further research activity in this or relevant areas.

Μέρος Α': Προβληματική και Πλαίσιο

Κεφάλαιο 1: Εισαγωγή

Κεφάλαιο 2: Η τεχνολογία Υποδομής Δημόσιου Κλειδιού και 3G Περιβάλλοντα:

Εννοιολογικό πλαίσιο

Κεφάλαιο 1: Εισαγωγή

1.1. Εισαγωγή

Κοινή διαπίστωση αποτελεί στις μέρες μας, ότι η «βιομηχανία» των κινητών τηλεπικοινωνιών βρίσκεται σε μια διαρκή μεταβολή και ενσωματώνει διαρκώς όλο και μεγαλύτερο αριθμό υπηρεσιών, τις οποίες προσφέρει στους χρήστες της. Οι υπηρεσίες αυτές προσφέρονται από διαρκώς αυξανόμενους σε πλήθος παρόχους (providers), ενώ εκρηκτική είναι και η αύξηση του αριθμού των συνδρομητών. Ενδεικτικό είναι ότι στο τέλος του έτους 2000 ο αριθμός των συνδρομητών κινητής τηλεφωνίας ξεπέρασε τα 700 εκατομμύρια, ενώ περισσότερα από 8 δισεκατομμύρια SMS μηνύματα στάλθηκαν μόνο κατά το μήνα Ιούνιο του ίδιου έτους. Στην Ιαπωνία η υπηρεσία *i-mode* είχε το έτος 2001 περίπου 17 εκατομμύρια συνδρομητές, οι οποίοι αυξάνονταν με ρυθμό 1 εκατομμύριο το μήνα. Η γνωστή εταιρεία Sony-Ericsson εκτιμά ότι στο τέλος του 2005 θα υπάρχουν πάνω από 1,6 δισεκατομμύρια χρήστες, από τους οποίους 1 δισεκατομμύριο θα χρησιμοποιούν τις υπηρεσίες κινητού διαδικτύου (mobile Internet) (Frodich et al., 2001). Τα σημαντικότερα αίτια είναι η γεωγραφική εξάπλωση των σχετικών υποδομών, η σημαντική μείωση του κόστους αλλά και η βελτίωση της ποιότητας των προσφερόμενων υπηρεσιών.

Ειδικότερα, η κινητή τηλεφωνία στον Ευρωπαϊκό χώρο ξεκίνησε στη Γερμανία το 1958 με το αναλογικό δίκτυο A-Netz χρησιμοποιώντας τη συχνότητα των 160 MHz. Το 1971 το σύστημα αυτό κάλυπτε γεωγραφικά το 80% και είχε 11.000 συνδρομητές. Το 1972 το παραπάνω δίκτυο εξελίχθηκε στο B-Netz χρησιμοποιώντας την ίδια συχνότητα. Το σύστημα ήταν επίσης διαθέσιμο στην Αυστρία, Λουξεμβούργο και Ολλανδία, ενώ μόνο στη Δυτική Γερμανία το 1979 είχε 13.000 συνδρομητές. Οι συσκευές (πομπός και δέκτης), λόγω του βάρους τους, ήταν συνήθως εγκατεστημένες μέσα σε κάποιο αυτοκίνητο. Το ίδιο διάστημα στις Βόρειες Ευρωπαϊκές χώρες (Δανία, Νορβηγία, Φιλανδία και Σουηδία) αναπτύχθηκε το αναλογικό σύστημα NMT (Nordic Mobile Telephone) στη συχνότητα των 450 MHz. Αρκετά ακόμη αναλογικά συστήματα κινητής τηλεφωνίας αναπτύχθηκαν μέχρι το 1980 στον Ευρωπαϊκό χώρο, τα οποία όμως χρησιμοποιούσαν τελείως διαφορετικά και ασύμβατα πρότυπα. Τα παραπάνω συστήματα είναι γνωστά ως η $1^{η}$ γενιά κινητών επικοινωνιών (1G).

Οι Ευρωπαϊκές χώρες συμφώνησαν να αναπτύξουν ένα πανευρωπαϊκό σύστημα ή πρότυπο κινητής τηλεφωνίας το 1982. Το νέο σύστημα θα χρησιμοποιούσε το νέο φάσμα των 900 MHz και θα επέτρεπε τη μεταγωγή κλήσεων μεταξύ των Ευρωπαϊκών χωρών. Επιπλέον, θα

ήταν πλήρως ψηφιακό και θα πρόσφερε τόσο φωνητικές όσο και υπηρεσίες δεδομένων. Το αποτέλεσμα αυτής της προσπάθειας κατέληξε στο σύστημα δεύτερης γενιάς κινητών επικοινωνιών (2G) ευρύτερα γνωστό ως GSM (Global System for Mobile Communication). Το GSM βασίζεται στην τεχνολογία Time Division Multiple Access (TDMA), λειτουργεί στις συχνότητες των 900 και 1800 MHz και ξεκίνησε τη λειτουργία του το έτος 1991.

Τα συστήματα 2G πρόσφεραν και συνεχίζουν να προσφέρουν μεγαλύτερη χωρητικότητα (capacity) δικτύου, χαμηλότερα κόστη στους παρόχους, ενώ χαμηλού ρυθμού (low-rate) υπηρεσίες δεδομένων προστέθηκαν στις φωνητικές υπηρεσίες. Ένα άλλο πλεονέκτημα των συστημάτων GSM είναι η ευρεία - σε όλο σχεδόν τον πλανήτη - δυνατότητα περιαγωγής (roaming). Άλλα συστήματα 2G, εκτός του GSM, είναι τα TDMA, Personal Digital Cellular (PDC) και cdmaOne. Το PDC χρησιμοποιείται στην Ιαπωνία, ενώ όλα τα υπόλοιπα συμπεριλαμβανομένου και του GSM, λειτουργούν στις Ηνωμένες Πολιτείες. Η εξέλιξη των συστημάτων 2G ώστε να συμπεριλάβουν υπηρεσίες δεδομένων (packet-switched data services) έγινε γνωστή και ως 2.5 γενιά κινητών επικοινωνιών (2.5G). Στα συστήματα GSM η υπηρεσία δεδομένων ονομάζεται General Packet Radio Service (GPRS). Το GPRS μπορεί να προσφέρει ρυθμούς δεδομένων πάνω από 20 Kb/s για κάθε χρονοθυρίδα (time slot).

Το 1992 η Ευρωπαϊκή Ένωση συμφώνησε στην ανάπτυξη του συστήματος τρίτης γενιάς (3G) με το όνομα UMTS (Universal Mobile Telecommunications System) ως πρόταση στη Διεθνή Ένωση Τηλεπικοινωνιών ITU (International Telecommunication Union) για το IMT-2000 (ITU-R, 2000). Τα συστήματα 3G αναπτύσσονται και προτυποποιούνται από δύο οργανισμούς γνωστούς ως 3rd Generation Partnership Project (3GPP) (www.3gpp.org) και 3GPP2 (www.3gpp2.org). Ο πρώτος οργανισμός ασχολείται με την εξέλιξη των συστημάτων GSM, ενώ ο δεύτερος με την εξέλιξη του συστήματος cdmaOne. Χρήσιμες πληροφορίες για τη δράση, τα κοινά σημεία και τις διαφορές των δύο οργανισμών αναφέρονται στο (Patel & Dennett, 2000). Κοινός στόχος και των δύο οργανισμών είναι η εξέλιξη των δικτύων των παρόχων ώστε να βασίζονται αποκλειστικά στο πρωτόκολλο IP (*all-IP*). Τα 3GPP δίκτυα λειτουργούν στη συχνότητα των 5MHz, βασίζονται στην τεχνολογία Wideband CDMA (W-CDMA) και προσφέρουν ρυθμούς δεδομένων από 144 kb/s για κινητούς σταθμούς (vehicular), 384 kb/s για ακίνητους σταθμούς (pedestrian) και 2 Mb/s για εσωτερικούς χώρους (indoor environments).

1.2. Ασφάλεια κινητών επικοινωνιών

Η ασφάλεια (security) των εκπεμπόμενων δεδομένων (data) αλλά και της σηματοδοσίας (signaling) αποτελεί ουσιώδες κεφάλαιο σε ένα σύστημα κινητών επικοινωνιών. Σε ζητήματα ασφάλειας πληροφοριών, τα ασύρματα δίκτυα είναι περισσότερο ευάλωτα σε επιθέσεις σε σχέση με τα ενσύρματα. Σε ένα ασύρματο δίκτυο η πρόσβαση δεν μπορεί να περιοριστεί σε

φυσικά καθορισμένο χώρο (physically). Επιπλέον, τα εκπεμπόμενα δεδομένα των χρηστών αλλά και της σηματοδοσίας μεταξύ δικτύου και των τερματικών κινητών σταθμών μπορούν να ληφθούν από οποιοδήποτε διαθέτει έναν κατάλληλο δέκτη. Κατά συνέπεια, είναι απαραίτητο να χρησιμοποιηθούν κατάλληλοι μηχανισμοί προστασίας, όπως κρυπτογραφικές τεχνικές, προκειμένου να προστατέψουν κατάλληλα τα δεδομένα, τη σηματοδοσία αλλά και τους πόρους του δικτύου.

Τα θέματα που κρίνεται απαραίτητο να αντιμετωπιστούν είναι η εμπιστευτικότητα (confidentiality) η ακεραιότητα (integrity) και η διαθεσιμότητα (availability) των δεδομένων και των υπηρεσιών του δικτύου. Πολύ σημαντικό είναι επίσης το ζήτημα της αναγνώρισης (identification) και πιστοποίησης της ταυτότητας των χρηστών, του δικτύου και των δεδομένων (authentication).

Όπως ήδη αναφέρθηκε, τα συστήματα 3G θα είναι βασισμένα αποκλειστικά στο πρωτόκολλο IP (all-IP). Παράλληλα, σε εξέλιξη βρίσκονται ερευνητικές προσπάθειες για την πλήρη ενοποίηση όλων των ασύρματων και ενσύρματων συστημάτων διαφορετικών τεχνολογιών (heterogeneous) σε ένα κοινό περιβάλλον, με στόχο την παροχή υψηλής ποιότητας υπηρεσιών στους συνδρομητές ανεξάρτητα από τη γεωγραφική περιοχή που αυτοί θα κινούνται. Αυτή η προοπτική εξέλιξης - προς την ενοποίηση των συστημάτων επικοινωνίας - είναι γνωστή ως η $4^{η}$ γενιά κινητών επικοινωνιών (4G).

Από τη πλευρά της ασφάλειας, η χρήση του πρωτοκόλλου IP δημιουργεί ακόμη περισσότερους κινδύνους. Τα δίκτυα των παρόχων 2G θεωρούνταν κλειστά (closed), εφόσον διέθεταν μικρή διασύνδεση με δίκτυα άλλων παρόχων ή με το Διαδίκτυο (Internet). Παρόλα αυτά, η διασύνδεση των δικτύων 3G με το Διαδίκτυο και με ετερογενή δίκτυα άλλων παρόχων βρίσκεται σε πλήρη εξέλιξη, ενώ το *all-IP* μοντέλο οδηγεί σε πολύπλοκες σχέσεις εμπιστοσύνης (trust) του τύπου πολλά προς πολλά (*many-to-many*) μεταξύ των διαφορετικών παρόχων. Κατά συνέπεια, οι τελευταίοι θα κληθούν να αντιμετωπίσουν σοβαρές απειλές για την ασφάλεια των δικτύων τους. Η επιτυχής ή όχι αντιμετώπισή τους θα επηρεάσει και την ποιότητα των προσφερόμενων υπηρεσιών στους τελικούς χρήστες.

1.3. Αφορμή και κίνητρα για την παρούσα έρευνα

Τα ζητήματα που αφορούν την ασφάλεια πληροφοριακών συστημάτων βρίσκονται ολοένα και περισσότερο στο επίκεντρο της κοινής γνώμης και των μέσων μαζικής ενημέρωσης. Παράλληλα, η επιστημονική έρευνα στο χώρο αυτό βρίσκεται σε διαρκή ανάπτυξη, δίνοντας ιδιαίτερη έμφαση σε ανάπτυξη τεχνικών, πρωτοκόλλων και μέσων προστασίας.

Παρά την ανάπτυξη νέων τεχνικών και εργαλείων ασφαλείας, τα επεισόδια ασφάλειας (security incidents) αλλά και οι κίνδυνοι δε φαίνεται να μειώνονται. Αντίθετα, νέες απειλές κάνουν

καθημερινά την εμφάνισή τους. Όπως ήδη αναφέρθηκε, τα συστήματα κινητών επικοινωνιών αντιμετωπίζουν περισσότερες απειλές σε σχέση με τα ενσύρματα. Παράλληλα, η ανάπτυξη και εξέλιξη των συστημάτων 3G σε αυτά της 4G αναμένεται να οξύνει πολύ περισσότερο αυτή την κατάσταση. Οι μελετητές της ασφάλειας των συστημάτων αυτών τονίζουν την ανάγκη για νέες ή βελτιωμένες τεχνικές και μεθόδους προστασίας, αναγνωρίζοντας τις επικείμενες απειλές (3GPP TS, 2000).

Συγκεκριμένα, αφορμή για την παρούσα έρευνα αποτέλεσαν οι εξής διαπιστώσεις:

- Οι αδυναμίες και τα κενά ασφάλειας που υπάρχουν στα 2G συστήματα, ορισμένα από τα οποία φαίνεται να διατηρούνται και στα αντίστοιχα 3G. Αυτό συμβαίνει γιατί η ανάπτυξη των 3G βασίστηκε σε μεγάλο βαθμό στα υπάρχοντα 2G συστήματα.
- Η εξέλιξη των συστημάτων 3G σε *all-IP* επιφέρει πλήθος νέων απειλών, πολλές από τις οποίες αντιμετωπίζουν ήδη τα ενσύρματα δίκτυα.
- Το μεγάλο πλήθος των διαφορετικών παρόχων, η ενοποίηση με το Internet και η διαδικτύωση με ασύρματα δίκτυα διαφορετικών τεχνολογιών, στοχεύει μεν σε υπηρεσίες 4G, αλλά παράλληλα δημιουργεί ένα πολύπλοκο μοντέλο σχέσεων εμπιστοσύνης μεταξύ των παρόχων, το οποίο απαιτεί συγκεκριμένες λύσεις σε θέματα ασφάλειας.
- Μεσοπρόθεσμα, η διαφαινόμενη αύξηση του αριθμού των παρόχων και των συνδρομητών τους απαιτεί εύκολα κλιμακούμενες λύσεις ασφαλείας, οι οποίες μέχρι στιγμής δε φαίνεται να συμπεριλαμβάνονται στα σχέδια των οργανισμών προτυποποίησης.
- Η αντιμετώπιση των κινδύνων που αναμένεται να αντιμετωπίσουν τα δίκτυα 3G και 4G θα πρέπει να προσανατολίζεται περισσότερο σε δοκιμασμένα εργαλεία και τεχνικές ασφαλείας και όχι σε μονοσήμαντες επιλογές, οι οποίες φαίνεται να συντηρούνται για χάρη συμβατότητας με τα συστήματα 2G.

1.4. Αντικείμενο και στόχοι της διατριβής

Αντικείμενο της παρούσας διατριβής είναι η αξιοποίηση της τεχνολογίας Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure, PKI) για την παροχή αξιόπιστων και ισχυρών μηχανισμών ασφάλειας στα κινητά δίκτυα επικοινωνιών τρίτης και μετέπειτα γενεών (beyond-3G, B3G). Σημειώνεται ότι η ερευνητική προσπάθεια εστιάζει στα 3G δίκτυα που προτυποποιούνται από τη 3GPP (UMTS). Παρόλα αυτά ο αναγνώστης μπορεί να εντοπίσει κοινά στοιχεία με τα δίκτυα CDMA2000 τα οποία αναπτύσσονται από τη 3GPP2. Σκοπός της έρευνας είναι να σχεδιάσει, να προτείνει και να αξιολογήσει την απόδοση λύσεων ασφαλείας που βασίζονται στην τεχνολογία δημόσιου κλειδιού και καλύπτουν τις ανάγκες των δικτύων 3G και B3G.

Τα κύρια ζητήματα στα οποία επικεντρώθηκε η έρευνα και παρουσιάζονται στην παρούσα διατριβή είναι:

- Να επισημάνει τα οφέλη της εισαγωγής της τεχνολογίας δημόσιου κλειδιού στα δίκτυα 3G και B3G, σε σχέση με το υπάρχον (3GPP) πλαίσιο.
- Να μελετήσει τρόπους ενσωμάτωσης της τεχνολογίας δημόσιου κλειδιού στα κεντρικά (core) δίκτυα των παρόχων υπηρεσιών 3G.
- Να σχεδιάσει, να μελετήσει και να αξιολογήσει λύσεις ασφαλείας, που μπορεί να προσφέρει μια PKI και μπορούν να εφαρμοστούν στα δίκτυα 3G και B3G.

Οι στόχοι της παρούσας έρευνας είναι:

- Να προτείνει και να αξιολογήσει τρόπους εισαγωγής της τεχνολογίας δημόσιου κλειδιού στα κεντρικά δίκτυα των παρόχων υπηρεσιών 3G και B3G.
- Να προτείνει και να αξιολογήσει λύσεις προσανατολισμένες σε PKI (PKI-oriented) με σκοπό την ενδο-δικτυακή (intra-network) και δια-δικτυακή (inter-network) προστασία των κεντρικών δικτύων των παρόχων υπηρεσιών 3G και B3G.
- Να προτείνει και να αξιολογήσει την απόδοση γνωστών πρωτοκόλλων δημόσιου κλειδιού, με σκοπό την παροχή αξιόπιστων υπηρεσιών αυθεντικοποίησης χρηστών σε περιβάλλοντα 3G και B3G.
- Να προτείνει και να αξιολογήσει την απόδοση άλλων πρόσθετων υπηρεσιών που προκύπτουν από την ενσωμάτωση της τεχνολογίας PKI στα δίκτυα αρχιτεκτονικής 3G και B3G.

1.5. Δομή της διατριβής

Η παρούσα διατριβή χωρίζεται σε τρία μέρη και επτά κεφάλαια (βλ. πίνακα 1-1). Στο πρώτο μέρος διαμορφώνεται το εννοιολογικό και επιστημολογικό υπόβαθρο, το οποίο είναι απαραίτητο για την κατανόηση της οπτικής μέσα από την οποία αντιμετωπίζεται το ζήτημα εισαγωγής της τεχνολογίας υποδομής δημόσιου κλειδιού στα δίκτυα κινητών επικοινωνιών τρίτης και ύστερων γενεών. Ακόμη, παρουσιάζονται τα κύρια σημεία προβληματισμού που οδήγησαν στην ενασχόληση με τα συγκεκριμένα ερευνητικά ζητήματα, ενώ ταξινομούνται και αναλύονται τα μέχρι στιγμής ερευνητικά δεδομένα.

Στο δεύτερο μέρος, αναλύονται και παρουσιάζονται συγκεκριμένες υπηρεσίες, οι οποίες πηγάζουν από τη χρήση τεχνολογίας δημόσιου κλειδιού και έχουν ως στόχο τόσο τους συνδρομητές όσο και τους παρόχους των δικτύων κινητών επικοινωνιών τρίτης και ύστερων γενεών. Η ανάλυση εστιάζεται στην εξασφάλιση των δια-δικτυακών και ενδο-δικτυακών επικοινωνιών των δικτύων των 3GPP παρόχων και σε ζητήματα αυθεντικοποίησης και εξουσιοδότη-

σης των συνδρομητών. Οι παραπάνω υπηρεσίες αναπτύσσονται και παράλληλα αξιολογούνται, αξιοποιώντας κατάλληλες αρχιτεκτονικές ενσωμάτωσης της τεχνολογίας PKI σε 3GPP περιβάλλοντα. Το τρίτο μέρος ολοκληρώνει τη διατριβή, παρουσιάζοντας γενικά συμπεράσματα που προκύπτουν από την παρούσα έρευνα και εξετάζει τις πιθανές προοπτικές για παραπέρα ερευνητική δραστηριοποίηση.

Μέρη – Κεφάλαια	**Κύριοι στόχοι**
Μέρος Α': Προβληματική και Εννοιολογικό πλαίσιο **Κεφ.1**: Εισαγωγή **Κεφ.2**: Η τεχνολογία Υποδομής Δημόσιου Κλειδιού και 3G Περιβάλλοντα: Εννοιολογικό πλαίσιο	✓ Οριοθέτηση της περιοχής επικέντρωσης. ✓ Ανάπτυξη εννοιολογικού υποβάθρου. Ορισμός των χρησιμοποιούμενων εννοιών. ✓ Υποστήριξη της κύριας ερευνητικής εργασίας που παρουσιάζεται στο δεύτερο μέρος. ✓ Κριτική θεώρηση της τρέχουσας έρευνας στην περιοχή επικέντρωσης. ✓ Μελέτη τρόπων ενσωμάτωσης της τεχνολογίας PKI στα 3G και B3G δίκτυα.
Μέρος Β': Ανάπτυξη και Αξιολόγηση υπηρεσιών **Κεφ.3**: Αξιοποίηση υπηρεσιών PKI για την εξασφάλιση ενδο-δικτυακών επικοινωνιών στα 3G και B3G δίκτυα. **Κεφ.4**: Αυθεντικοποίηση χρηστών 3G και B3G με χρήση πρωτοκόλλων δημόσιου κλειδιού και υποστήριξη PKI. **Κεφ.5**: Αυθεντικοποίηση χρηστών σε ετερογενή δικτυακά περιβάλλοντα WLAN-3G με χρήση τεχνολογίας PKI. **Κεφ.6**: Παροχή ψηφιακών πιστοποιητικών ιδιοτήτων σε χρήστες ετερογενών δικτύων WLAN-3G.	✓ Να προτείνει και να αξιολογήσει, σε σχέση με το ισχύον πλαίσιο, τρόπους αξιοποίησης της τεχνολογίας PKI, με σκοπό την εξασφάλιση των ενδο-δικτυακών και δια-δικτυακών επικοινωνιών στα κεντρικά δίκτυα των 3G και B3G παρόχων. ✓ Να προτείνει και να αξιολογήσει συγκεκριμένους μηχανισμούς αυθεντικοποίησης που βασίζονται σε δημόσια κρυπτοσυστήματα για τους συνδρομητές 3G και B3G-υβριδικών αρχιτεκτονικών. ✓ Να προτείνει νέες, προστιθέμενης αξίας PKI-υπηρεσίες και αρχιτεκτονικές ενσωμάτωσής τους σε 3G και B3G περιβάλλοντα και να αξιολογήσει την απόδοση και αποτελεσματικότητά τους.
Μέρος Γ': Επίλογος **Κεφ.7**: Συμπεράσματα και προοπτικές περαιτέρω έρευνας.	✓ Συνοπτική παρουσίαση των γενικών συμπερασμάτων που προκύπτουν από την παρούσα έρευνα και εξέταση των προοπτικών συνέχισής της.

Πίνακας 1-1. Δομή της διατριβής

1.6. Συμβολή της διατριβής

Με την παρούσα διατριβή επιχειρείται ο σχεδιασμός, η αξιοποίηση και η αξιολόγηση της τεχνολογίας υποδομής δημόσιου κλειδιού, για την παροχή αξιόπιστων, ισχυρών, ευέλικτων και κλιμακούμενων μηχανισμών ασφαλείας στους συνδρομητές και στους παρόχους 3GPP και 3GPP/WLAN ετερογενών περιβαλλόντων. Η συνεισφορά της διατριβής ανά κεφάλαιο παρουσιάζεται αναλυτικά στον πίνακα 1-2.

Κεφάλαια	Συμβολή της διατριβής
Κεφάλαιο 1	
Κεφάλαιο 2	Επισκόπηση της τρέχουσας έρευνας και διερεύνηση των μεθόδων ενσωμάτωσης της τεχνολογίας PKI στην υπάρχουσα αρχιτεκτονική πυρήνα των 3GPP δικτύων (Kambourakis et al., 2002; Kambourakis et al., 2004b).
Κεφάλαιο 3	Ανάπτυξη και συγκριτική αξιολόγηση προτάσεων για παροχή ισχυρών, αξιόπιστων και κλιμακούμενων μηχανισμών ενδο-δικτυακής και δια-δικτυακής ασφάλειας στα δίκτυα 3G, αξιοποιώντας υποδομές δημόσιου κλειδιού (Kambourakis et al., 2003; Kambourakis et al., 2004).
Κεφάλαιο 4	Αξιοποίηση, ανάπτυξη και αξιολόγηση της αποδοτικότητας των υπηρεσιών PKI για την παροχή ευέλικτων και ισχυρών μηχανισμών αυθεντικοποίησης των συνδρομητών των 3GPP δικτύων (Kambourakis et al., 2004c; Kambourakis et al. 2004d).
Κεφάλαιο 5	Αξιοποίηση και αξιολόγηση της αποδοτικότητας των υπηρεσιών PKI για παροχή ισχυρών και κλιμακούμενων μηχανισμών αυθεντικοποίησης των συνδρομητών υβριδικών 3GPP-WLAN περιβαλλόντων (Kambourakis et al., 2004e; Kambourakis et al., 2004f).
Κεφάλαιο 6	Ανάπτυξη αξιολόγηση της αποδοτικότητας κατάλληλης δικτυακής αρχιτεκτονικής με στοιχεία PKI, για την παροχή και διαχείριση ψηφιακών πιστοποιητικών στους χρήστες ετερογενών δικτύων 3GPP-WLAN (Kambourakis et al., 2004b; Kambourakis et al., 2004g; Kambourakis et al., 2004h).
Κεφάλαιο 7	Περιγραφή ανοικτών ερευνητικών ζητημάτων που προκύπτουν από την παρούσα διδακτορική έρευνα.

Πίνακας 1-2. Συμβολή της διατριβής ανά κεφάλαιο

Κεφάλαιο 2: Τεχνολογία Υποδομής Δημόσιου Κλειδιού και 3G περιβάλλοντα: Εννοιολογικό Πλαίσιο

2.1. Εισαγωγή στην Τεχνολογία Δημόσιου Κλειδιού

2.1.1. Γενικά

Η γνωστική περιοχή της ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων τα τελευταία χρόνια παρουσιάζει σημαντική ερευνητική ένταση, ιδιαίτερα στην ανάπτυξη τεχνικών και μέσων προστασίας από κακόβουλες ή μη επιθέσεις. Τα κρυπτοσυστήματα δημόσιου κλειδιού (Public Key Cryptosystem), (Diffie & Hellman, 1976; Rivest et al., 1978; Oppliger, 2002) προϋποθέτουν τη χρήση ενός ζεύγους κλειδιών, τα οποία συσχετίζονται μαθηματικά.

- Ένα Δημόσιο κλειδί (public key), το οποίο με διασφαλισμένη την ακεραιότητά του, μπορεί να δημοσιευτεί και να προσπελαστεί από όλους τους χρήστες του συστήματος.
- Ένα ιδιωτικό κλειδί (private key), το οποίο είναι γνωστό μόνο από το συγκεκριμένο χρήστη.

Επίσης, με βάση τα σημερινά τεχνολογικά δεδομένα, με κανένα τρόπο δεν είναι εφικτό να βρεθεί το ένα κλειδί ενώ είναι γνωστό το άλλο. Η λειτουργία ενός κρυπτοσυστήματος δημόσιου κλειδιού περιγράφεται με το παρακάτω παράδειγμα:

- Ο χρήστης Α και ο χρήστης Β κατέχουν από ένα ζεύγος κλειδιών $(K_\alpha, K_\alpha^{-1})$ και (K_β, K_β^{-1}), όπου K_α, K_β τα δημόσια και K_α^{-1}, K_β^{-1} τα ιδιωτικά κλειδιά των χρηστών.
- Αν ο Α επιθυμεί να στείλει κάποιο μήνυμα στο Β τότε χρησιμοποιεί το K_β και κρυπτογραφεί το μήνυμα.
- Όταν το μήνυμα παραληφθεί από το Β τότε αυτός χρησιμοποιώντας το K_β^{-1} το αποκρυπτογραφεί.
- Η αποκρυπτογράφηση δεν είναι δυνατή, αν τα κλειδιά δεν είναι από το ίδιο ζεύγος.

Υπάρχουν δύο βασικές προσεγγίσεις για τον τρόπο δημιουργίας του ζεύγους των κλειδιών. Η πρώτη βασίζεται στο κατανεμημένο (distributed) μοντέλο, δηλαδή ο κάθε χρήστης δημιουργεί το αντίστοιχο ζεύγος ιδιωτικού και δημόσιου κλειδιού. Κατόπιν, αποθηκεύει με ασφαλή τρόπο το ιδιωτικό κλειδί του τοπικά και αποστέλλει μια αίτηση δημιουργίας πιστοποιητικού

(βλ. ενότητα 2.1.3) μαζί με το δημόσιο κλειδί του στην CA, η οποία του επιστρέφει το σχετικό πιστοποιητικό δημόσιου κλειδιού (Public Key Certificate, PKC).

Εναλλακτικά, η διαδικασία δημιουργίας του ζεύγους των κλειδιών μπορεί να ακολουθεί το συγκεντρωτικό (centralized) μοντέλο. Σύμφωνα μ' αυτό, ένα κεντρικό σύστημα διαχείρισης κλειδιών (enterprise key administration center) δημιουργεί τα ζεύγη κλειδιών, αποστέλλει ανάλογες αιτήσεις στη συνεργαζόμενη CA για έκδοση πιστοποιητικών και επιστρέφει τα ιδιωτικά κλειδιά μαζί με τα PKCs στους δικαιούχους. Η λύση αυτή είναι, πολλές φορές, προτιμητέα έναντι της πρώτης, ειδικά σε περιπτώσεις, όπου είναι αναγκαία η διατήρηση αντιγράφων των κλειδιών για λόγους ασφαλείας.

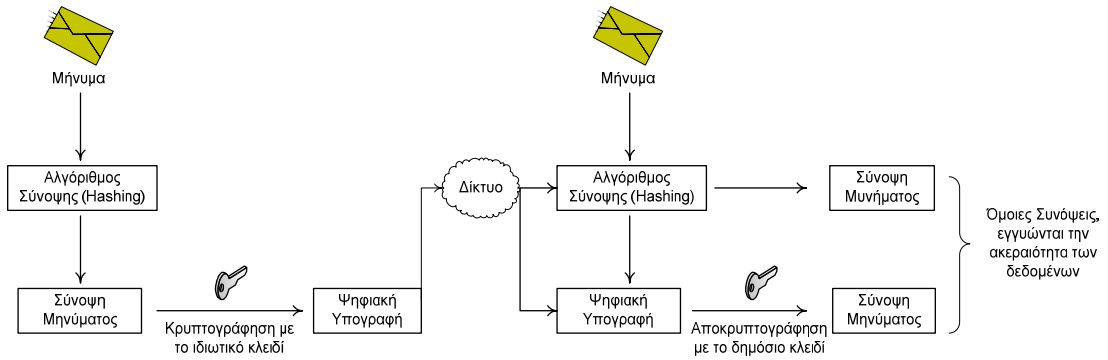
2.1.2. Ψηφιακές Υπογραφές (Digital Signatures)

Ένα κρυπτοσύστημα δημόσιων κλειδιών μπορεί να προστατέψει όχι μόνο την εμπιστευτικότητα (confidentiality) ενός μηνύματος, αλλά και την αυθεντικότητα (authenticity) και ακεραιότητά (integrity) του. Έτσι, στο παραπάνω παράδειγμα αν ο Α επιθυμεί να εξασφαλίσει την αυθεντικότητα ενός μηνύματος, θα δημιουργήσει μια ψηφιακή υπογραφή του. Οι ψηφιακές υπογραφές παρέχουν ένα ψηφιακό ανάλογο των ιδιόχειρων υπογραφών και γι' αυτό:

- Η αντιγραφή τους πρέπει να είναι αδύνατη.
- Οι παραλήπτες πρέπει να είναι σε θέση να τις επιβεβαιώσουν
- Οι υπογράφοντες δεν είναι δυνατό να αρνηθούν πως υπέγραψαν σε μεταγενέστερο χρόνο, διασφαλίζοντας τη μη-αποποίηση (non-repudiation).

Μία σημαντική διαφορά σε σχέση με τις παραδοσιακές υπογραφές είναι πως μια ψηφιακή υπογραφή δεν είναι μοναδική αλλά είναι συνάρτηση του μηνύματος που αυτή υπογράφει. Διαφορετικά θα ήταν εύκολη η αντιγραφή και επικόλλησή της σε διαφορετικά μηνύματα. Στην ουσία, λοιπόν, η χρήση ψηφιακών υπογραφών προϋποθέτει (βλ. σχήμα 2-1):

- Έναν αλγόριθμο παραγωγής κλειδιών, ο οποίος επιλέγει τυχαία ένα ζεύγος (δημόσιο, ιδιωτικό).
- Έναν αλγόριθμο υπογραφής, ο οποίος δέχεται ως δεδομένα ένα μήνυμα και ένα ιδιωτικό κλειδί και επιστρέφει ως αποτέλεσμα μια ψηφιακή υπογραφή για το μήνυμα.
- Έναν αλγόριθμο επαλήθευσης ψηφιακής υπογραφής, ο οποίος δέχεται ως δεδομένα μία ψηφιακή υπογραφή και ένα δημόσιο κλειδί και επιστρέφει ως αποτελέσματα ένα μήνυμα και ένα δυαδικό ψηφίο (bit) που δείχνει αν η υπογραφή είναι αυθεντική.



Σχήμα 2-1. Δημιουργία και επιβεβαίωση ψηφιακής υπογραφής

2.1.3. Ψηφιακά Πιστοποιητικά (Digital Certificates)

Θα μπορούσε κάποιος να αναρωτηθεί με ποιο τρόπο όμως ο Α μπορεί να γνωρίζει ότι το δημόσιο κλειδί για τον Β που υπάρχει π.χ. σε μια βάση, ανήκει πράγματι στον Β και όχι σε κάποιον που τον υποδύεται. Για να αντιμετωπίσει ένα κρυπτοσύστημα δημόσιων κλειδιών το πρόβλημα της αυθεντικοποίησης (Authentication) των χρηστών χρησιμοποιεί ψηφιακά πιστοποιητικά δημόσιου κλειδιού (PKCs). Ένα PKC είναι μια δομή δεδομένων που χρησιμοποιείται για να δηλώσει την ταυτότητα κάποιου - ή κάποιας οντότητας γενικά – (server, εταιρείας) και συσχετίζει μοναδικά την οντότητα αυτή με ένα δημόσιο κλειδί.

Οι Αρχές Πιστοποίησης (Certification Authorities, CAs), είναι οντότητες οι οποίες πιστοποιούν την ταυτότητα κάποιου και εκδίδουν το σχετικό PKC. Αυτές μπορεί να είναι Έμπιστες Τρίτες Οντότητες (Trusted Third Parties, TTP), ονομαζόμενες και Πάροχοι Υπηρεσιών Πιστοποίησης (Certification Service Providers, CSP) ή οργανισμοί, οι οποίοι εκτελούν το δικό τους λογισμικό έκδοσης πιστοποιητικών. Το έργο της πιστοποίησης μπορεί να ανατίθεται, για λόγους εξισορρόπησης φόρτου, σε μια Αρχή Εγγραφής (Registration Authority, RA).

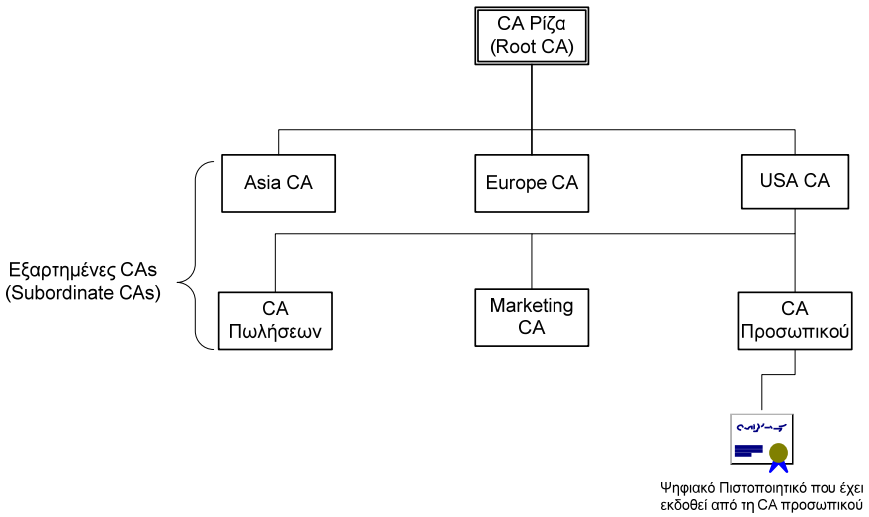
Ένα PKC σύμφωνα με το πρότυπο X.509 (ITU-T, 1997) περιέχει διάφορα στοιχεία – πεδία όπως: το όνομα και το δημόσιο κλειδί της οντότητας που πιστοποιεί την ταυτότητά της, ημερομηνίες έκδοσης και λήξης, ένα σειριακό αριθμό, το όνομα της οντότητας που υπογράφει το πιστοποιητικό κ.α. Το πλέον σημαντικό, όμως, είναι πως κάθε PKC φέρει τη ψηφιακή υπογραφή της CA που το εκδίδει – γεγονός που εξασφαλίζει την ακεραιότητα και αυθεντικότητά (authenticity) του.

Γενικότερα, ο όρος «πιστοποιητικό» αναφέρεται σε ένα ψηφιακά υπογεγραμμένο αποδεικτικό, το οποίο παραχωρεί σε αυτόν που το κατέχει κάποια δικαιώματα ή προνόμια. Μια περίπτωση, όπως είδαμε, είναι το πιστοποιητικό να περιέχει το δημόσιο κλειδί της οντότητας στο οποίο αναφέρεται. Ένα πιστοποιητικό μπορεί, επίσης, να εκχωρεί μερικά γενικά χαρακτηριστικά (attributes) στον ιδιοκτήτη του. Για παράδειγμα, να εκχωρεί το δικαίωμα του «διάβασε» ή του «διάβασε – γράψε» σε μια βάση δεδομένων. Σ' αυτή την περίπτωση τα πιστοποιη-

τικά ονομάζονται Πιστοποιητικά Ιδιοτήτων (Attribute Certificates, AC), ενώ οι αρχές που τα εκδίδουν Αρχές πιστοποίησης ιδιοτήτων (Attributes Authorities, AA) (Farrell & Housley, 2002; Housley & Polk, 2001).

2.1.4. Ιεραρχίες Αρχών Πιστοποίησης (CA Hierarchies)

Σε μεγάλους οργανισμούς, ίσως είναι αναγκαία η μεταβίβαση της ευθύνης έκδοσης PKCs σε διαφορετικές CAs. Όταν για παράδειγμα, ο αριθμός των πιστοποιητικών που απαιτούνται είναι πολύ μεγάλος για να τον διαχειριστεί μια και μόνο CA, ή στην περίπτωση όπου διαφορετικές γεωγραφικά περιοχές ή ακόμα και τμήματα μιας μεγάλης επιχείρησης, έχουν διαφορετικές πολιτικές έκδοσης πιστοποιητικών. Το πρότυπο X.509 περιέχει ένα μοντέλο για τη δημιουργία μιας ιεραρχίας CAs, όπως αυτή που παρουσιάζεται στο σχήμα 2-2.

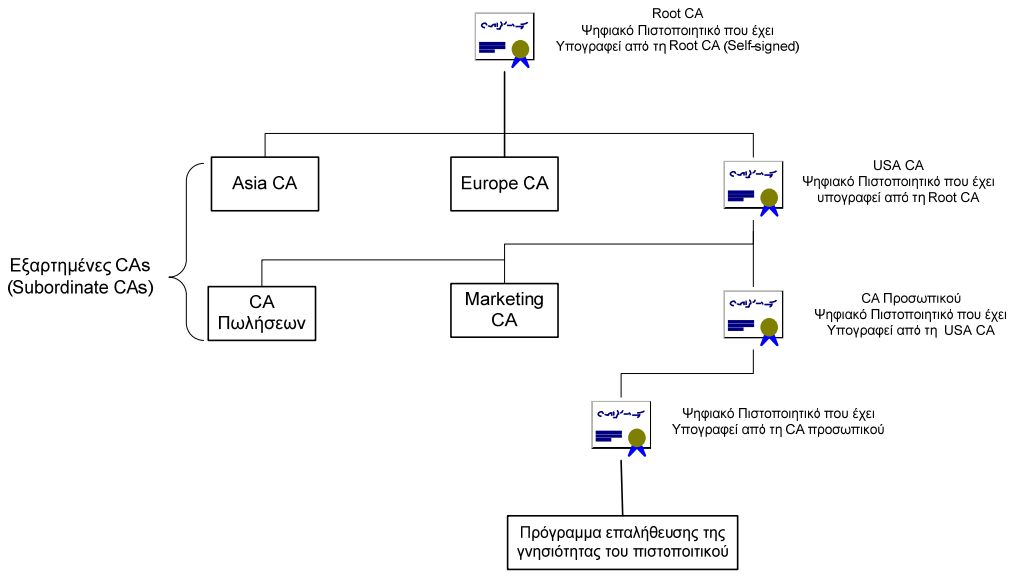


Σχήμα 2-2. Ιεραρχία αρχών Πιστοποίησης

Όπως παρατηρούμε, η CA ρίζα (Root CA) βρίσκεται στην κορυφή της ιεραρχίας. Το PKC της root CA έχει υπογραφεί από την ίδια (self-signed). Τα πιστοποιητικά των CA που βρίσκονται στο αμέσως επόμενο επίπεδο, υπογράφονται από τη ρίζα κ.ο.κ.

2.1.5. Αλυσίδες Πιστοποιητικών (Certificate Chains)

Οι ιεραρχίες CAs αντικατοπτρίζονται στις αλυσίδες πιστοποιητικών. Μία αλυσίδα πιστοποιητικών είναι μια σειρά από PKCs που έχουν εκδοθεί από διαδοχικές (ιεραρχικά) CA. Στο σχήμα 2-3, φαίνεται μια αλυσίδα πιστοποιητικών που πιστοποιούν μια οντότητα διαμέσου δύο εξαρτημένων αρχών πιστοποίησης (subordinate CAs) και της ρίζας.



Σχήμα 2-3. Αλυσίδες Πιστοποιητικών

Σε μια αλυσίδα πιστοποιητικών ισχύουν τα παρακάτω:

- Κάθε πιστοποιητικό ακολουθείται από το πιστοποιητικό της CA που το εκδίδει.
- Κάθε πιστοποιητικό περιέχει το όνομα (Distinguish Name, DN) αυτού που το εκδίδει, το οποίο είναι όμοιο με το επόμενο πιστοποιητικό στην αλυσίδα (από κάτω προς τα πάνω).
- Κάθε πιστοποιητικό υπογράφεται ψηφιακά με το ιδιωτικό κλειδί του εκδότη. Η υπογραφή μπορεί να επιβεβαιωθεί μόνο με το δημόσιο κλειδί του εκδότη, το οποίο είναι το επόμενο (από κάτω προς τα πάνω) πιστοποιητικό στην αλυσίδα. Για παράδειγμα, στο σχήμα 2-3 το δημόσιο κλειδί στο πιστοποιητικό για τη USA CA, μπορεί να χρησιμοποιηθεί για να επαληθεύσει την ψηφιακή υπογραφή της USA CA, στο πιστοποιητικό για την CA πωλήσεων.

2.1.6. Υποδομή Δημόσιου Κλειδιού (PKI)

Διαφαίνεται λοιπόν, η ανάγκη για την ύπαρξη μιας υποδομής για την υποστήριξη των κρυπτοσυστημάτων δημόσιων κλειδιών. Ως υποδομή ασφάλειας δημόσιου κλειδιού (PKI) ορίζουμε το σύνολο του υλικού, λογισμικού, ανθρώπων, πολιτικών και διαδικασιών που απαιτούνται για τη δημιουργία, αποθήκευση, διαχείριση, διανομή και κατάργηση πιστοποιητικών βασισμένων στην κρυπτογραφία με τη χρήση δημόσιων κλειδιών (IETF PKIX, 2004; Adams & Lloyd, 1999; Nash et al. 2001; Housley & Polk, 2001). Στη γενική της μορφή μια PKI αποτελείται από πέντε τύπους οντοτήτων:

- CAs οι οποίες εκδίδουν και καταργούν PKCs.
- RAs, οι οποίες εγγυώνται για την αντιστοίχιση μεταξύ των δημόσιων κλειδιών και των κατόχων των πιστοποιητικών ή άλλων χαρακτηριστικών – δικαιωμάτων.

- Κάτοχοι PKCs, οι οποίοι μπορούν να υπογράφουν ψηφιακά έγγραφα και να τα κρυπτογραφούν.
- Πελάτες (clients), οι οποίοι επαληθεύουν ψηφιακές υπογραφές και / ή αλυσίδες πιστοποιητικών.
- Αποθήκες πιστοποιητικών (Certificate Repositories, CR), οι οποίες αποθηκεύουν και διανέμουν PKCs και λίστες ανακληθέντων πιστοποιητικών (λίστες με πιστοποιητικά που έχουν λήξει – Certificate Revocation Lists, CRL).

2.2. Συστήματα κινητών επικοινωνιών & PKI

2.2.1. Η 2η Γενιά κινητών επικοινωνιών

Τα χαρακτηριστικά ασφάλειας των συστημάτων κινητών επικοινωνιών δεύτερης γενιάς (2G/2.5G), όπως το GSM, βασίζονται στη χρήση συμμετρικής κρυπτογραφίας (Symmetric Cryptography). Ο πάροχος (provider) υπηρεσιών κινητών επικοινωνιών (Public Land Mobile Network operator, PLMN), παραχωρεί στον κάθε χρήστη του δικτύου του μια έξυπνη κάρτα (smart card), η οποία ονομάζεται Στοιχείο Αναγνώρισης Συνδρομητή (Subscriber Identity Module, SIM). Στην κάρτα αυτή είναι αποθηκευμένο ένα, μοναδικό για κάθε συνδρομητή, μυστικό κλειδί το οποίο χρησιμοποιείται για να αυθεντικοποιείται ο συνδρομητής στο δίκτυο. Το ίδιο κλειδί, είναι αποθηκευμένο και στο κέντρο αυθεντικοποίησης συνδρομητών (Authentication Centre, AuC) του PLMN.

Πρέπει να σημειωθεί, ότι κατά τη διαδικασία αυθεντικοποίησης, η οποία λαμβάνει χώρα, όταν ο συνδρομητής ανοίγει το κινητό του τηλέφωνο, μόνον ο χρήστης ή καλύτερα, ο κινητός εξοπλισμός του χρήστη (User Equipment, UE), αυθεντικοποιείται στο δίκτυο. Αντίθετα, το δίκτυο δεν αυθεντικοποιείται στο συνδρομητή. Σημαντικό ζήτημα επίσης, είναι η πλήρης έλλειψη μέτρων ενδο-δικτυακής (intra-network) και δια-δικτυακής (inter-network) προστασίας στα δίκτυα 2G. Εξαιτίας των παραπάνω, αλλά και άλλων αδυναμιών ασφαλείας (3GPP TS, 2000), η $2^{η}$ γενιά δικτύων κινητών επικοινωνιών παρέχει πρόσφορο έδαφος στους εν δυνάμει επιτιθέμενους (attackers). Για παράδειγμα, πολύ γνωστοί τύποι επιθέσεων που αφορούν 2G συστήματα, είναι η κλωνοποίηση (cloning) SIM, οι επιθέσεις τύπου man-in-the-middle (MITM) κ.α.

Κατά τη διάρκεια του σχεδιασμού της αρχιτεκτονικής ασφαλείας των συστημάτων αυτών, η ιδέα για χρήση δημόσιων κλειδιών και PKI είχε απορριφθεί. Αιτίες ήταν ο αυξημένος υπολογιστικός φόρτος που απαιτεί η εφαρμογή κρυπτογραφικών τεχνικών δημόσιου κλειδιού, ειδικά από την πλευρά των ΜΕ των χρηστών, καθώς και το σημαντικό κόστος υλοποίησης. Παρόλα αυτά, με την πρόοδο που σημειώθηκε στην κρυπτογραφία και στην τεχνολογία κρυπτο-

γραφικής επεξεργασίας (αλγόριθμοι λιγότερο απαιτητικοί σε υπολογιστικούς πόρους), η υπολογιστική επιβάρυνση μπορεί να μην αποτελεί πλέον σημαντικό περιοριστικό παράγοντα για τα μελλοντικά συστήματα κινητών επικοινωνιών.

2.2.2. Η 3η Γενιά κινητών επικοινωνιών

Το 1988 συστάθηκε ο υπεύθυνος οργανισμός ο οποίος ανέλαβε το έργο ανάπτυξης, εξέλιξης και προτυποποίησης των συστημάτων 3G, με την επωνυμία 3rd Generation Partnership Project (3GPP). Σήμερα, βρισκόμαστε στην αρχή της εγκατάστασης και λειτουργίας συστημάτων 3G, ενώ η διαδικασία ορισμού των τεχνικών προδιαγραφών από την 3GPP βρίσκεται στην έκδοση 6 (Release 6). Το σύστημα που προτυποποιείται από τη 3GPP είναι γνωστό και ως Universal Mobile Telecommunication System (UMTS).

Η 3η γενιά κινητών επικοινωνιών, αν και χαρακτηρίζεται από πολλές βελτιώσεις σε ζητήματα ασφάλειας που εντοπίζονται στη 2η γενιά, εξακολουθεί να παρουσιάζει αρκετά κενά ή αδύνατα σημεία. Σημαντικές βελτιώσεις για παράδειγμα, αποτελούν η αμοιβαία αυθεντικοποίηση χρηστών – δικτύου και η πρόβλεψη μηχανισμών ενδο-δικτυακής και δια-δικτυακής ασφάλειας. Παράλληλα, η διαδικασία ορισμού τεχνικών προδιαγραφών για αρκετά θέματα, όπως αυτό της συνεργασίας 3GPP δικτύων και άλλου τύπου ασύρματων τοπικών δικτύων (Wireless LAN, WLAN) βρίσκεται σε διαδικασία εξέλιξης.

Βασικός στόχος των σχεδιαστών του νέου συστήματος ήταν να διατηρήσουν τη μέγιστη δυνατή συμβατότητα με τα συστήματα 2ης γενιάς. Η επιλογή αυτή, καθώς και οι περιορισμοί σε υπολογιστικό φόρτο και κόστος που αναφέρθηκαν στην προηγούμενη ενότητα, οδήγησαν εκ νέου τη 3GPP να απομακρυνθεί από λύσεις και υπηρεσίες PKI. Παρόλα αυτά, ερευνητικά έργα (projects), όπως το ASPeCT (ASPeCT, 1999) και το USECA (USECA, 1999), είχαν καταδείξει ότι η εφαρμογή μεθόδων και λύσεων δημόσιου κλειδιού ήταν δυνατό να προσφέρει ισχυρές και εφαρμόσιμες υπολογιστικά υπηρεσίες ασφάλειας στα 3G συστήματα. Παράλληλα, έγγραφα προς συζήτηση του οργανισμού 3GPP (3GPP TSG 2001; 3GPP TSG 2001a; 3GPP TSG, 2002) ειδικά μετά την έκδοση 5, όπως και άλλες ερευνητικές εργασίες (Kambourakis et al. 2003; Grecas et al. 2003; Trask & Jaweed, 2001) προβλέπουν αυτή την εξέλιξη. Στη Νορβηγία, χώρα όπου οι υπηρεσίες κινητής τηλεφωνίας είναι πολύ διαδεδομένες, βρίσκεται σε εξέλιξη το έργο “eNorge 2005” (eNorge, 2002), το οποίο αφορά την ανάπτυξη ενός PKI για τη χώρα. Ακόμη, σύγχρονα πρότυπα (standards) όπως το MexE, WAP (WAP Forum, 2001) και το *i-mode* από την εταιρεία NTT DoCoMo έχουν προχωρήσει στην εισαγωγή μεθόδων και τεχνολογίας PKI. Επίσης, επιτυχημένες υλοποιήσεις ασύρματων PKI (wireless PKI) από γνωστές εταιρείες του χώρου όπως η Sonera Smarttrust και η Lucent Technologies, ενδυναμώνουν την άποψη ότι η τεχνολογία PKI υπόσχεται την παροχή αξιόπιστων λύσεων για μελλοντικά συστήματα κινητών επικοινωνιών.

Επιπλέον, είναι γνωστό ότι η ασύμμετρη κατανομή φορτίου μπορεί να βοηθήσει να μειωθούν τα προβλήματα υπολογιστικού φόρτου που σχετίζονται με τη χρήση μηχανισμών κρυπτογραφίας δημόσιου κλειδιού. Για παράδειγμα, τα πρωτόκολλα επικοινωνίας μπορούν να σχεδιαστούν έτσι ώστε οι κρυπτογραφικές λειτουργίες ιδιαίτερα από την πλευρά του τελικού χρήστη (end-user) να είναι λιγότερο απαιτητικές από αυτές που θα εκτελούνται από την πλευρά του δικτύου. Επίσης, τα συστήματα χρήσης μηχανισμών δημόσιου κλειδιού απαιτούν μικρότερο άμεσης πρόσβασης (on-line) χρόνο αλληλεπίδρασης μεταξύ του δικτύου εξυπηρέτησης (Serving Network, SN) και του δικτύου που ανήκει ο συνδρομητής (Home Network, HN), σε σχέση με αντίστοιχα που χρησιμοποιούν συμμετρικό κλειδί.

Πρέπει επίσης να σημειωθεί ότι η εφαρμογή PKI λύσεων μπορεί να προσφέρει σημαντικά πλεονεκτήματα τόσο στον ίδιο τον πάροχο όσο και στους τελικούς χρήστες. Η εύκολη κλιμάκωση σε ένα περιβάλλον που χαρακτηρίζεται από σχέσεις τύπου πολλά προς πολλά, η απ' άκρο σ' άκρο (end-to-end) ασφάλεια των επικοινωνιών, αλλά και άλλες επιπρόσθετες υπηρεσίες, όπως η μη-αποποίηση των συναλλαγών και η παροχή πιστοποιητικών ιδιοτήτων, καλλιεργούν το έδαφος για την ενσωμάτωση τεχνολογίας PKI στα 3G περιβάλλοντα.

Η αντίστοιχη της SIM κάρτας του GSM στο σύστημα UMTS, ονομάζεται Universal Subscriber Identity Module (USIM). Παρόλα αυτά, στο UMTS η USIM είναι καλύτερο να εννοείται ως εφαρμογή (application) και όχι ως υλικό-κάρτα (hardware). Για την ίδια την κάρτα, χρησιμοποιείται ο όρος Universal Integrated Circuit Chip (UICC). Είναι ενδεικτικό, ότι μια UICC μπορεί να περιέχει πολλές USIM εφαρμογές. Για παράδειγμα, μπορεί να επιτρέπει στο χρήστη της να χρησιμοποιεί εναλλακτικά τα συστήματα UMTS και CDMA2000 ενώ ταξιδεύει, να υποστηρίζει διαδικασίες αυθεντικοποίησης σε WLAN δίκτυα, να περιέχει τα δημόσια και ιδιωτικά κλειδιά του συνδρομητή, να δημιουργεί ψηφιακές υπογραφές κ.ά.

2.3. Απαιτήσεις εισαγωγής τεχνολογίας PKI σε 3G δίκτυα

2.3.1. Γενικές απαιτήσεις

Υπάρχουν δύο δυνατότητες για την ενσωμάτωση μιας PKI στα δίκτυα 3G:

- Η PKI ενσωματώνεται στο κεντρικό δίκτυο του παρόχου και λειτουργεί υπό την επίβλεψή του.
- Η PKI είναι εγκατεστημένη εκτός του κεντρικού δικτύου του παρόχου και λειτουργεί ως TTP/CSP. Αυτό συνεπάγεται την ύπαρξη συγκεκριμένης συμφωνίας παροχής υπηρεσιών (service agreement) μεταξύ του παρόχου 3G και του TTP/CSP.

Ανεξάρτητα από τη λύση που επιλέγει να εφαρμόσει ο εκάστοτε πάροχος, η εισαγωγή μιας PKI απαιτεί τα παρακάτω:

1. Την ύπαρξη τουλάχιστον μιας CA, η οποία εκδίδει (issue) και ανακαλεί (revoke) ψηφιακά πιστοποιητικά. Μια RA μπορεί να υποστηρίζει το έργο της CA, προσφέροντας υπηρεσίες εγγραφής και αυθεντικοποίησης (Nash et al., 2001). Αν ο πάροχος σκοπεύει να προσφέρει και πιστοποιητικά ιδιοτήτων, τότε μπορεί να χρησιμοποιηθεί ξεχωριστή AA ή η λειτουργία της να ενσωματωθεί στην CA.

2. Web ή FTP εξυπηρέτες μπορούν να χρησιμοποιηθούν για την αποθήκευση των ψηφιακών πιστοποιητικών και των λιστών ανακληθέντων πιστοποιητικών (Certificates Revocation Lists, CRL). Η ανάκληση πιστοποιητικών μπορεί να γίνεται περιοδικά ή με βάση το πρωτόκολλο Online Certificate Status Protocol (OCSP) (Iliadis et al., 2003).

3. Η UICC κάρτα του κάθε συνδρομητή αποθηκεύει με ασφαλή τρόπο (tamper-resistant) το ιδιωτικό και το δημόσιο κλειδί του μαζί με το αντίστοιχο PKC. Υπάρχει βέβαια η δυνατότητα για χρήση από τον εκάστοτε συνδρομητή περισσότερων του ενός ζεύγους κλειδιών και πιστοποιητικών, ανάλογα με την περίπτωση. Επίσης, στην κάρτα μπορεί να αποθηκεύονται τα PKC (ή τα δημόσια κλειδιά) όλων των CAs που συνεργάζονται με ή ανήκουν στο συγκεκριμένο πάροχο. Ο τρόπος με τον οποίο η λειτουργία μιας UICC και μιας Secure Signature Creation Device (SSCD), που διατηρεί το(α) ιδιωτικό(α) κλειδί(α) ενός συνδρομητή μπορούν να συνδυαστούν και ο τρόπος με τον οποίο τα κλειδιά αυτά μπορούν να αποκτηθούν κατά περίπτωση (on-demand) χωρίς τη μεσολάβηση του παρόχου αναλύεται στα (Rossnagel, 2004; WAP Forum, 2001).

4. Επιπλέον, η κάρτα UICC αποθηκεύει όλα τα πιστοποιητικά ρίζας των CAs που υπάρχουν στο κεντρικό δίκτυο του συγκεκριμένου παρόχου ή συνεργάζονται μ' αυτόν.

5. Κάθε στοιχείο του κεντρικού δικτύου του παρόχου διατηρεί ένα παρόμοιο ζεύγος κλειδιών και το αντίστοιχο PKC.

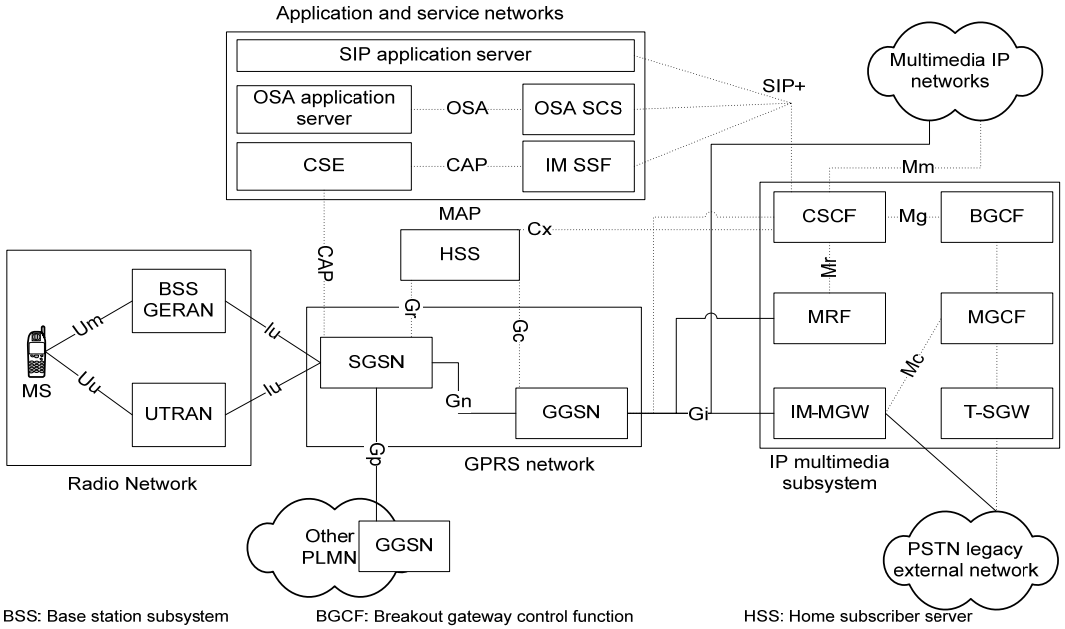
6. Υπάρχει τουλάχιστον μια αποθήκη πιστοποιητικών (Certificates Repository, CR), η οποία αποθηκεύει όλα τα ψηφιακά πιστοποιητικά που εκδίδονται στο χώρο ευθύνης του παρόχου.

Πρόσθετες λειτουργικές απαιτήσεις, όπου αυτές είναι απαραίτητες, αναφέρονται στα επόμενα κεφάλαια (βλ. ενότητες 3.2.3, 4.2 και 6.2).

2.3.2. Απαιτήσεις στην αρχιτεκτονική του δικτύου 3G

Μία γενική απεικόνιση της 3GPP αρχιτεκτονικής (3GPP TS, 2003; Lin et al. 2002) παρουσιάζεται στο σχήμα 2-4. Όπως ήδη έχει αναφερθεί στα προηγούμενα, η ενοποίηση 3GPP δικτύων και PKI δεν έχει ακόμη προτυποποιηθεί. Τουλάχιστον τέσσερις εναλλακτικές λύσεις μπορούν να προταθούν (Kambourakis et al., 2004b; 3GPP TSG, 2002b). Δύο από αυτές παρουσιάζονται στο σχήμα 2-5, ενώ οι υπόλοιπες θα αναπτυχθούν στα Κεφάλαια 3 και 6 αντί-

στοιχα. Σε κάθε περίπτωση, μια PKI θα πρέπει να μπορεί να προσφέρει διάφορες υπηρεσίες (έκδοση πιστοποιητικών, υπηρεσίες μη-αποποίησης κτλ) τόσο στον τελικό χρήστη, όσο και στο ίδιο το δίκτυο του παρόχου (έκδοση και ανάκληση πιστοποιητικών για τα στοιχεία του δικτύου). Ειδικά για τους χρήστες, οι PKI υπηρεσίες θα πρέπει να παρέχονται, είτε αυτοί βρίσκονται στο HN είτε σε κάποιο άλλο δίκτυο που έχει συνάψει και διατηρεί κάποια συμφωνία μεταγωγής (Roaming Agreement, RoA) με το HN.



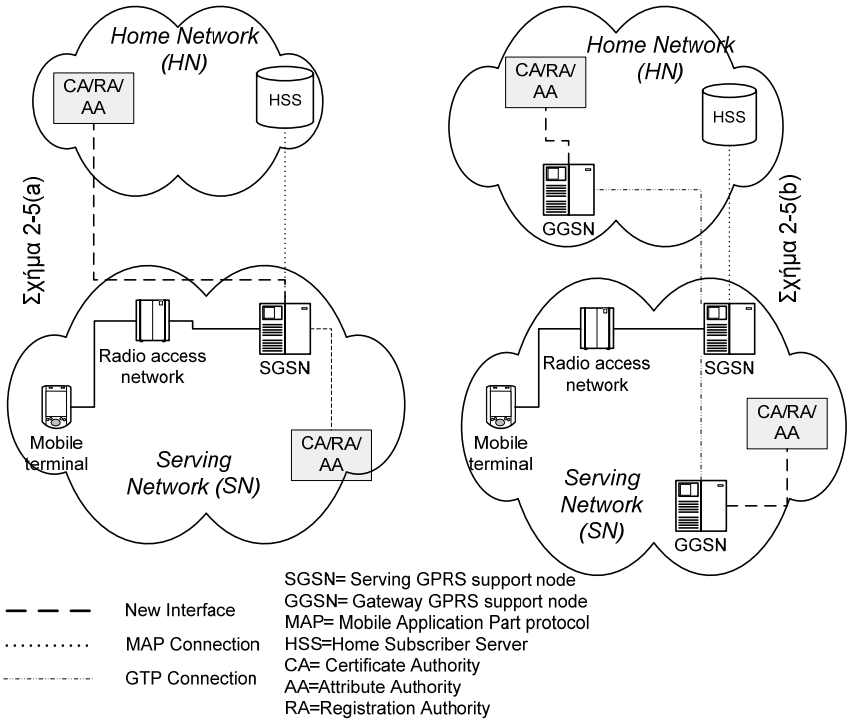
Σχήμα 2-4. Γενική άποψη UMTS all-IP αρχιτεκτονικής έκδοσης 6.0

Στο σχήμα 2-5(a), η CA συνδέεται πάντα στο SGSN του HN, ενώ στο σχήμα 2-5(b), η CA συνδέεται στο τοπικό GGSN. Και στις δύο περιπτώσεις όλα τα PKI στοιχεία (elements), υποθέτουμε ότι αποτελούν τμήμα του κεντρικού δικτύου του παρόχου, επομένως προστατεύονται από τους εκάστοτε ισχύοντες μηχανισμούς ασφαλείας του (Network Domain Security, NDS). Η σύνδεση των PKI οντοτήτων με τα SGSN ή GGSN είναι βασισμένη στο πρωτόκολλο IP. Επιπλέον, και οι δύο λύσεις απαιτούν προτυποποίηση νέων μηνυμάτων σηματοδοσίας μεταξύ των επικοινωνούντων στοιχείων (CA, SGSN/GGSN).

Οι προτεινόμενες επιλογές παρουσιάζουν μειονεκτήματα αλλά και πλεονεκτήματα. Για παράδειγμα, για την αρχιτεκτονική που παρουσιάζεται στα αριστερά, η διαδικασία εύρεσης της διεύθυνσης της CA είναι εύκολη, μιας και η CA είναι πάντα συνδεδεμένη στο SGSN του SN, ενώ δεν απαιτείται ο ορισμός νέων διαδικασιών ασφαλείας μεταξύ του SGSN και των συσκευών των τελικών χρηστών (User Equipment, UE). Απ' την άλλη πλευρά, πρέπει να ορι-

στεί μια νέα διεπαφή (interface) μεταξύ των παρόχων (inter-operator), δηλαδή μεταξύ του SGSN του SN και του HN. Επιπλέον, η προσπέλαση της CA του HN, όταν ο χρήστης περιάγει (roams), απαιτεί για παράδειγμα, να υπάρχει η διεύθυνσή της αποθηκευμένη στη UE.

Η αρχιτεκτονική του σχήματος 2-5(b), ίσως αποτελεί την πιο ενδιαφέρουσα λύση, γιατί το GGSN είναι η υπεύθυνη οντότητα (entity) για την επικοινωνία με στοιχεία που βρίσκονται εκτός του IP υποσυστήματος (IP-subsystem) του HN του παρόχου. Αυτό είναι ιδιαίτερα βολικό, σε περίπτωση όπου η PKI δεν αποτελεί τμήμα του κεντρικού δικτύου (core network) του παρόχου αλλά συνεργαζόμενη οντότητα, όπως είδαμε στην ενότητα 2.3.1. Ως μειονέκτημα θα πρέπει να σημειώσουμε την ανάγκη προτυποποίησης νέων μηνυμάτων σηματοδοσίας μεταξύ UE – GGSN και SGSN – GGSN.



Σχήμα 2-5. Εναλλακτικές αρχιτεκτονικές για την ενοποίηση 3GPP δικτύων και PKI

2.4. Σύνοψη – Συμπεράσματα

Συνοψίζοντας μπορούμε να καταλήξουμε στις εξής παρατηρήσεις:

- Τα δίκτυα 3G ακολουθώντας τη λογική της συμβατότητας με αυτά της 2G, δε συμπεριέλαβαν στον αρχικό σχεδιασμό τους λύσεις ασφάλειας βασισμένες σε PKI.
- Αρκετά ερευνητικά έργα και άρθρα είχαν και έχουν ως θέμα τους τη σκοπιμότητα εισαγωγής της τεχνολογίας δημόσιου κλειδιού στα κινητά δίκτυα 3^{ης} γενιάς. Παράλληλα, επιτυχημένες υλοποιήσεις ασύρματων PKI ισχυροποιούν την άποψη για σύγκλιση των δύο τεχνολογιών.

- Υπάρχουν αρκετές εναλλακτικές λύσεις ενσωμάτωσης της τεχνολογίας PKI στα δίκτυα 3G. Όλες παρουσιάζουν μειονεκτήματα και πλεονεκτήματα, τα οποία πρέπει να αξιολογηθούν κατά περίπτωση.

Μέρος Β': Ανάπτυξη και Αξιολόγηση Υπηρεσιών

Κεφάλαιο 3: Αξιοποίηση υπηρεσιών PKI για την εξασφάλιση ενδο-δικτυακών και δια-δικτυακών επικοινωνιών στα 3G και B3G δίκτυα.

Κεφάλαιο 4: Αυθεντικοποίηση χρηστών 3G και B3G με χρήση πρωτοκόλλων δημόσιου κλειδιού και υποστήριξη PKI.

Κεφάλαιο 5: Αυθεντικοποίηση χρηστών σε ετερογενή δικτυακά περιβάλλοντα WLAN-3G με χρήση τεχνολογίας PKI.

Κεφάλαιο 6: Παροχή ψηφιακών πιστοποιητικών ιδιοτήτων σε χρήστες ετερογενών δικτύων WLAN-3G.

Κεφάλαιο 3: Αξιοποίηση υπηρεσιών PKI για την εξασφάλιση ενδο-δικτυακών και δια-δικτυακών επικοινωνιών στα 3G και B3G δίκτυα.

3.1. Εισαγωγή

Είναι γνωστό, πως το κεντρικό (core) δίκτυο των παρόχων υπηρεσιών 2G χαρακτηρίζεται από απουσία μηχανισμών ασφάλειας. Για παράδειγμα, ενώ χρησιμοποιούνται κλειδιά κρυπτογράφησης για να προστατέψουν τα εκπεμπόμενα δεδομένα μεταξύ χρηστών και δικτύου, αυτά τα κλειδιά μεταφέρονται απροστάτευτα (unprotected) μεταξύ των κεντρικών δικτύων διαφορετικών παρόχων. Αρχικά, και έως την έκδοση 99 του UMTS, το γεγονός αυτό δεν αποτελούσε ιδιαίτερο πρόβλημα, μιας και τα 2G κεντρικά δίκτυα χρησιμοποιούν για τις ανάγκες σηματοδοσίας μεταξύ των οντοτήτων του δικτύου το πρωτόκολλο Signaling System No 7 (SS7). Έτσι, κατά κανόνα, τα δίκτυα αυτά θεωρούνταν «κλειστά» (closed) με μικρή διασύνδεση με δίκτυα άλλων παρόχων και το Διαδίκτυο.

Όμως, η ίδια λογική δεν είναι δυνατό να εφαρμοστεί και στα δίκτυα 3G και B3G. Αυτά θα απαιτούν συχνές διασυνδέσεις με τα δίκτυα άλλων παρόχων, τα οποία μάλιστα μπορεί να είναι διαφορετικών τεχνολογιών (WLAN, 3GPP2). Επιπλέον, η εισαγωγή του IP πρωτοκόλλου για τις ανάγκες σηματοδοσίας και μεταφοράς των δεδομένων των χρηστών, όπως στο GPRS, καθιστά επιτακτική την ανάγκη για ισχυρούς μηχανισμούς προστασίας.

Τα 3GPP δίκτυα μέχρι την έκδοση 6, χρησιμοποιούν αποκλειστικά συμμετρικές (symmetric key) μεθόδους για τις διαδικασίες αυθεντικοποίησης των χρηστών, κρυπτογράφησης της σηματοδοσίας και των δεδομένων και την προστασία της ακεραιότητάς τους. Παρόλα αυτά, το επικοινωνιακό μοντέλο (2G) πρόσωπο-με-πρόσωπο (*person-to-person*) πρόκειται σύντομα να μεταβληθεί σε μοντέλο (4G) μηχανή-προς-μηχανή (*machine-to-machine*). Κατά συνέπεια, απαιτούνται περισσότερο ευέλικτοι (flexible), ευπροσαρμόσιμοι (reconfigurable) και κλιμακούμενοι (scalable) μηχανισμοί ασφαλείας οι οποίοι μπορούν να εξυπηρετήσουν μοντέλα εμπιστοσύνης (trust) του τύπου πολλά-προς-πολλά.

Όπως είδαμε στο Κεφάλαιο 2, η τεχνολογία PKI, διεισδύει σιγά – σιγά στα δίκτυα κινητών επικοινωνιών, ενώ ήδη αποτελεί *de-facto* πρότυπο στον κόσμο των ενσύρματων δικτύων. Η ενσωμάτωση PKI τεχνολογίας στα 3G και B3G δίκτυα μπορεί να αντικαταστήσει τις μακροχρόνιες (long-term) σχέσεις εμπιστοσύνης που βασίζονται σε συμμετρικά κλειδιά, με ευέλι-

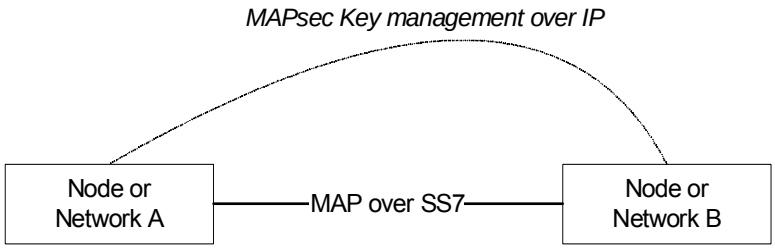
κτους, ευπροσαρμόσιμους και κλιμακούμενους μηχανισμούς ασφαλείας που μπορεί να προσφέρει ένα κρυπτοσύστημα δημόσιων κλειδιών. Στόχος είναι, η βελτίωση του επιπέδου εμπιστοσύνης μεταξύ των παρόχων, η διασφάλιση των επικοινωνιών εντός των κεντρικών δικτύων τους, η αύξηση της εμπιστοσύνης του χρήστη προς το δίκτυο και η προαγωγή λύσεων απ' άκρο σ' άκρο. Το παρόν κεφάλαιο ασχολείται με τη διασφάλιση των δια-δικτυακών και ενδο-δικτυακών επικοινωνιών των δικτύων των 3G ή B3G παρόχων, προτείνοντας λύσεις βασισμένες σε PKI. Αντίστοιχα θέματα μεταξύ τελικών χρηστών και 3G/B3G δικτύων θα εξεταστούν στα επόμενα κεφάλαια.

3.2. Πρότυπα ασφάλειας δικτύων 3GPP και PKI

3.2.1. Περιγραφή των 3GPP δια-δικτυακών και ενδο-δικτυακών μηχανισμών ασφαλείας

Η ανταλλαγή των μηνυμάτων σηματοδοσίας μεταξύ των στοιχείων του κεντρικού δικτύου στα συστήματα GSM και UMTS βασίζεται στο πρωτόκολλο Mobile Application Part (MAP). Για παράδειγμα, τα στοιχεία (profiles) των συνδρομητών, οι διαδικασίες αυθεντικοποίησης, και η διαχείριση της κινητικότητας (mobility) των χρηστών διεκπεραιώνονται μέσω του MAP. Τυπικά, το πρωτόκολλο MAP εκτελείται πάνω από τη στοίβα (stack) πρωτοκόλλων SS7. Για παράδειγμα, η σηματοδοσία μεταξύ του SGSN, του GGSN, της βάσης με τα στοιχεία των συνδρομητών (Home Subscriber Server, HSS) αλλά και του κέντρου διεκπεραίωσης SMS, βασίζεται αποκλειστικά σε SS7.

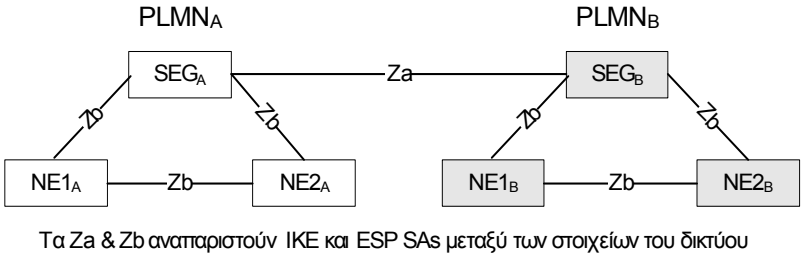
Η 3GPP έχει ορίσει ένα μηχανισμό για την προστασία του MAP πρωτοκόλλου στο επίπεδο εφαρμογής (application layer) (3GPP TS, 2002; Arkko & Blom, 2004). Το MAP μπορεί επίσης να προστατευτεί στο επίπεδο δικτύου (network layer), όταν η μεταφορά των δεδομένων βασίζεται στο πρωτόκολλο IP. Όμως, η προστασία του MAP στο επίπεδο εφαρμογής είναι υποχρεωτική, όταν απαιτείται δια-δικτύωση (interworking) με δίκτυα που βασίζονται σε SS7. Για την προστασία των MAP λειτουργιών έχει αναπτυχθεί μια νέα επικεφαλίδα πρωτοκόλλου (protocol header). Η λειτουργία της μοιάζει με αυτή του μηχανισμού Encapsulating Security Payload (ESP) του πρωτοκόλλου IPsec. Το νέο αυτό πρωτόκολλο ονομάζεται MAPsec και λειτουργεί σε τρεις καταστάσεις (modes). Στην κατάσταση 2, το MAPsec προστατεύει τόσο την εμπιστευτικότητα όσο και την ακεραιότητα των μηνυμάτων, ενώ στην κατάσταση 1 διασφαλίζεται μόνον η ακεραιότητα. Κανενός είδους προστασία δεν παρέχεται στην κατάσταση λειτουργίας 0. Ενώ τυπικά το MAP εκτελείται πάνω από SS7, το MAPsec και το πρωτόκολλο Internet Key Exchange (IKE) εκτελούνται πάντα πάνω από το IP, όπως φαίνεται στο σχήμα 3-1.



Σχήμα 3-1. Αρχιτεκτονική MAP

Είναι λοιπόν προφανές ότι οι δικτυακοί κόμβοι (nodes) που υποστηρίζουν το MAPsec, διατηρούν πάντα εκτός από SS7 και IP συνδεσιμότητα (connectivity). Στη 3GPP αρχιτεκτονική, το MAPsec τυπικά εκτελείται μεταξύ των δικτύων δύο διαφορετικών παρόχων. Οι ίδιες σχέσεις προστασίας (Security Associations, SA), χρησιμοποιούνται και από έναν αριθμό οντοτήτων των δύο δικτύων. Οι απαραίτητες MAPsec-SAs μεταξύ δικτύων διαφορετικών παρόχων είναι προϊόν διαπραγμάτευσης μεταξύ των αντίστοιχων Κέντρων Διαχείρισης Κλειδιών (Key Administration Centers, KAC) των δικτύων (Xenakis & Merakos, 2004).

Από την άλλη πλευρά, για τις IP δικτυακές οντότητες, όπως είναι η κορμός (backbone) του GPRS, οι μηχανισμοί ασφαλείας θα παρέχονται στο επίπεδο δικτύου. Τα πρωτόκολλα που θα χρησιμοποιηθούν είναι αυτά της σουίτας IPsec (Kent & Atkinson, 1998). Τα όρια (borders) μεταξύ των 3GPP δικτύων διαφορετικών παρόχων θα προστατεύονται από Πύλες Ασφαλείας (Security Gateways, SEG), όπως φαίνεται στο σχήμα 3-2. Έτσι, όλη η κίνηση δεδομένων και σηματοδοσίας μεταξύ διαφορετικών IP υποσυστημάτων θα διέρχεται μέσω μιας SEG πριν εισέλθει ή εγκαταλείψει το συγκεκριμένο τομέα ασφαλείας (security domain). Η ασφάλεια των δικτυακών IP υποσυστημάτων (Network Domain Security/IP) θα υποστηρίζει μόνο IPsec-SAs κατάστασης διόδου (tunneling), ESP και main mode. Οι SEGs θα προσφέρουν δυνατότητες για ασφαλή αποθήκευση μακροπρόθεσμων (long-term) συμμετρικών κλειδιών που θα χρησιμοποιούνται για αυθεντικοποίηση με βάση το πρωτόκολλο IKE. Τέλος, μόνον οι διαδικτυακές IKE-SA διαπραγματεύσεις (negotiations) πάνω από τις Za διασυνδέσεις θα είναι υποχρεωτικές, ενώ για τις Zb διασυνδέσεις η ευθύνη υλοποίησης θα ανήκει στον εκάστοτε πάροχο.



Σχήμα 3-2. Αρχιτεκτονική ασφαλείας μεταξύ IP υποσυστημάτων

3.2.2. PKI και Κινητά δίκτυα επικοινωνιών: Μια πραγματοποιήσιμη προοπτική

Όπως ήδη αναφέρθηκε, το βασικό εργαλείο για την προστασία των IP υποσυστημάτων σύμφωνα με τις 3GPP προτυποποιήσεις είναι το πρωτόκολλο IPsec. Το κρίσιμο σημείο αυτής της προσέγγισης είναι η διαχείριση των κλειδιών: Πώς αυτά δημιουργούνται, ανταλλάσσονται και διανέμονται ώστε να είναι διαθέσιμα από τους αλγορίθμους που παρέχουν υπηρεσίες εμπιστευτικότητας και ακεραιότητας των δεδομένων και της σηματοδοσίας. Προς το παρόν, τα κλειδιά και οι SAs, αποτελούν αντικείμενο διμερών συμφωνιών μεταξύ των διάφορων παρόχων.

Η ανάγκη για περισσότερο αποτελεσματικούς και κυρίως κλιμακούμενους μηχανισμούς ασφάλειας, οδηγεί στην αντικατάσταση των παραπάνω συμφωνιών με τεχνολογία PKI. Αυτό σημαίνει ότι οι επικοινωνίες μπορούν να εξασφαλιστούν χωρίς να υπάρχει η ανάγκη δημιουργίας και διανομής μακροπρόθεσμων συμμετρικών κλειδιών. Συγκρίνοντας ένα ασύμμετρο σύστημα κλειδιών με ένα συμμετρικό μπορούμε να σημειώσουμε τα παρακάτω:

- Ο αριθμός των κλειδιών που απαιτούνται από ένα συμμετρικό κρυπτοσύστημα για *n* επικοινωνούσες δικτυακές οντότητες είναι $O(n^2)$. Αντίστοιχα, για ένα κρυπτοσύστημα δημόσιων κλειδιών είναι $O(n)$. Όσο λοιπόν το *n* αυξάνει, τόσο τα κόστη για δημιουργία, διανομή και διαχείριση κλειδιών πολλαπλασιάζονται στην πρώτη περίπτωση. Όταν για παράδειγμα, προστίθεται ένα νέο στοιχείο (Network Element, NE) στο συμμετρικό μοντέλο χρειαζόμαστε n το πλήθος νέα κλειδιά, ενώ στο ασύμμετρο μόνο 2 νέα κλειδιά (ιδιωτικό & δημόσιο). Στην πραγματικότητα, σύγχρονες PKI υλοποιήσεις υποστηρίζουν ένα ή δύο ζεύγη κλειδιών για κάθε χρήστη. Τα συστήματα αυτά είναι γνωστά ως *single key pair* PKI και *dual key pair* PKI systems. Αυτό είναι ιδιαίτερα εξυπηρετικό σε περιπτώσεις όπου το ένα κλειδί χρησιμοποιείται από τις εφαρμογές μόνο για τη δημιουργία ψηφιακών υπογραφών, ενώ το άλλο μόνο για υπηρεσίες εμπιστευτικότητας.

- Τα προκαθορισμένα συμμετρικά κλειδιά δεν είναι ο καλύτερος τρόπος για την παροχή υπηρεσιών αυθεντικοποίησης. Αντίθετα, μια καλά σχεδιασμένη PKI, η οποία υποστηρίζει ψηφιακά πιστοποιητικά, μπορεί να προσφέρει περισσότερο δυναμικούς, ευέλικτους και κλιμακούμενους μηχανισμούς για την έκδοση και ανάκληση πιστοποιητικών σε νέες ή υπάρχουσες δικτυακές οντότητες.

- Μία βασική υπόθεση και απαίτηση στα συστήματα GSM και UMTS είναι ότι το HN πρέπει να εμπιστεύεται το SN. Όμως, η προβλεπόμενη στο μέλλον ύπαρξη πολλών συνεργαζόμενων δικτύων διαφόρων τεχνολογιών, τα οποία θα ανήκουν σε διαφορετικούς παρόχους, απαιτεί διαφορετική προσέγγιση. Με την εισαγωγή TTPs/CSPs μειώνονται αυτομάτως οι απαιτήσεις για διμερείς συμφωνίες μεταξύ των παρόχων.

- Μια PKI μπορεί να παρέχει υπηρεσίες αυθεντικοποίησης και ενθυλάκωσης - μεταφοράς (encapsulation) των συμμετρικών κλειδιών, ενώ τα τελευταία μπορούν να χρησιμοποιηθούν ως τα κύρια κλειδιά σε μια σύνοδο (session keys), παρέχοντας εμπιστευτικότητα.
- Από την πλευρά του τελικού χρήστη, η χρήση αλγορίθμων δημόσιου κλειδιού θεωρήθηκε σημαντικά πιο απαιτητική σε πόρους απ' αυτή των συμμετρικών μεθόδων. Το συγκεκριμένο πρόβλημα φαίνεται να αμβλύνεται, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις στο χώρο της τεχνολογίας των IP κινητών σταθμών, οι οποίοι πλέον ενσωματώνουν αρκετά ισχυρούς επεξεργαστές και σημαντικά μεγέθη μνήμης.
- Τα βασισμένα σε IP κινητά δίκτυα στοχεύουν στην εξυπηρέτηση μιας ποικιλίας εφαρμογών, οι οποίες μπορεί να εμπλέκουν πολλούς και διαφορετικούς παρόχους υπηρεσιών, σε ένα μοντέλο εμπιστοσύνης πολλά-προς-πολλά. Σε πολλές περιπτώσεις μάλιστα, οι επικοινωνούσες οντότητες μπορεί να μη διαθέτουν προ-συμφωνημένες διαδικασίες ασφάλειας. Σ' αυτή τη περίπτωση, για να είναι δυνατή η αυθεντικοποίηση και η δημιουργία συμμετρικών κλειδιών συνόδου για ασφαλή επικοινωνία μεταξύ των οντοτήτων, απαιτείται η υποστήριξη ψηφιακών υπογραφών και πιστοποιητικών μέσω εγκατεστημένων PKIs. Για παράδειγμα, ένας Session Initiation Protocol (SIP) εξυπηρέτης εγγραφής (registration server) μπορεί να μη μοιράζεται κάποιο συμμετρικό κλειδί με το UE. Αντ' αυτού, PKC και ψηφιακές υπογραφές μπορεί να χρησιμοποιηθούν για να παρέχουν υπηρεσίες αυθεντικοποίησης.

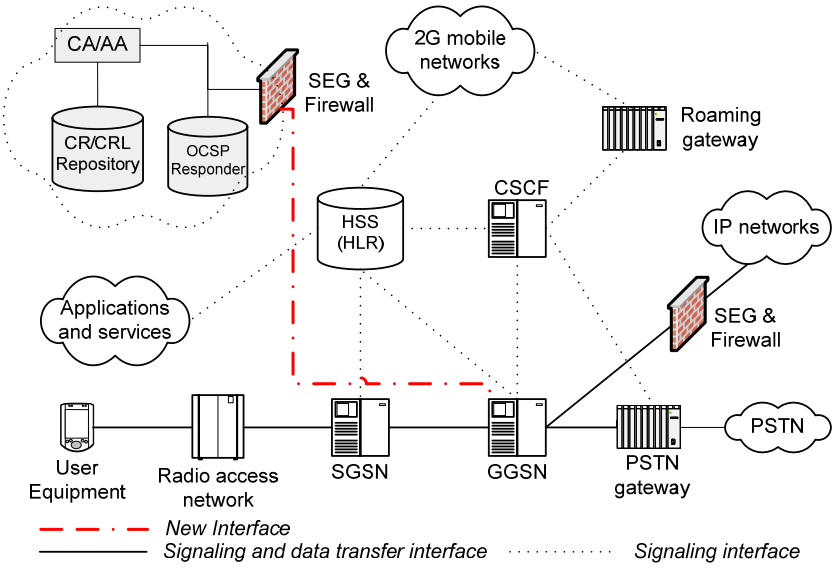
3.2.3. Προσαρμογή μιας PKI

Επιπλέον των προϋποθέσεων που αναφέρθηκαν στην ενότητα 2.3.1, απαιτούνται τα εξής:

1. Η ανάκληση πιστοποιητικών είναι γενικά ένα δύσκολο πρόβλημα το οποίο απαιτεί προσεκτική αντιμετώπιση. Σ' αυτή την περίπτωση, η ανάκληση πιστοποιητικών για τις οντότητες του κεντρικού δικτύου του παρόχου μπορεί να διενεργείται με μη-αυτόματο (manually) τρόπο. Αυτό δικαιολογείται από το γεγονός ότι η ανάκληση πιστοποιητικών για τα στοιχεία του δικτύου π.χ. GGSN είναι κάτι αρκετά σπάνιο (λόγω επισκευής, αντικατάστασης κτλ). Επιπλέον, η ανάκληση των πιστοποιητικών των συνδρομητών μπορεί να βασίζεται στο International Mobile Subscriber Identity (IMSI) (3GPP TS, 2002c).
2. Οι CAs, οι οποίες ανήκουν ή συνεργάζονται με διαφορετικούς παρόχους, μπορούν να αλληλο-πιστοποιηθούν (cross-reference), ανταλλάσσοντας πιστοποιητικά (Nash et al., 1999; 3GPP TSG, 2000). Για παράδειγμα, στην περίπτωση δύο παρόχων με δύο CAs, CAa & CAb αντίστοιχα, η CAa εκδίδει το $Cert(CAa)_{CAa}$ (το πιστοποιητικό ρίζας) και το $Cert(CAb)_{CAa}$. Αντίστοιχα, η CAb εκδίδει το $Cert(CAb)_{CAb}$ και το $Cert(CAa)_{CAb}$.

3. Τα cross-reference πιστοποιητικά αποθηκεύονται στις τοπικές SEGs, οι οποίες μπορεί να υλοποιούν και πολιτικές αναχώματος ασφαλείας (firewall). Κάθε πάροχος μπορεί να χρησιμοποιεί μια ή περισσότερες SEGs με σκοπό την ισορρόπηση του φόρτου κίνησης (traffic load) του δικτύου.

Μια λεπτομερέστερη αναπαράσταση της αρχιτεκτονικής του σχήματος 2-5 που παρουσιάστηκε στην ενότητα 2.3.2 παρουσιάζεται παρακάτω (βλ. σχήμα 3-3).



Σχήμα 3-3. Συνδυασμός 3GPP αρχιτεκτονικής έκδοσης 5 και PKI

3.3. Δια-δικτυακή και Ενδο-δικτυακή ασφάλεια βασισμένη σε PKI

3.3.1. IPsec, IKE και εγκαθίδρυση SAs

Ο όρος Network Domain Security (NDS), σημαίνει κυρίως ασφαλείς επικοινωνίες μεταξύ των στοιχείων ενός δικτύου. Η εισαγωγή τεχνολογίας PKI στα μελλοντικά δίκτυα κινητών επικοινωνιών, μπορεί να προσφέρει ισχυρά πρωτόκολλα για την προστασία της σηματοδοσίας και των δεδομένων που μεταφέρονται διαμέσου δια-δικτυακών και ενδο-δικτυακών συνδέσεων. Όπως φαίνεται στο σχήμα 3-2, δύο διασυνδέσεις (interfaces) θα πρέπει να προστατευτούν:

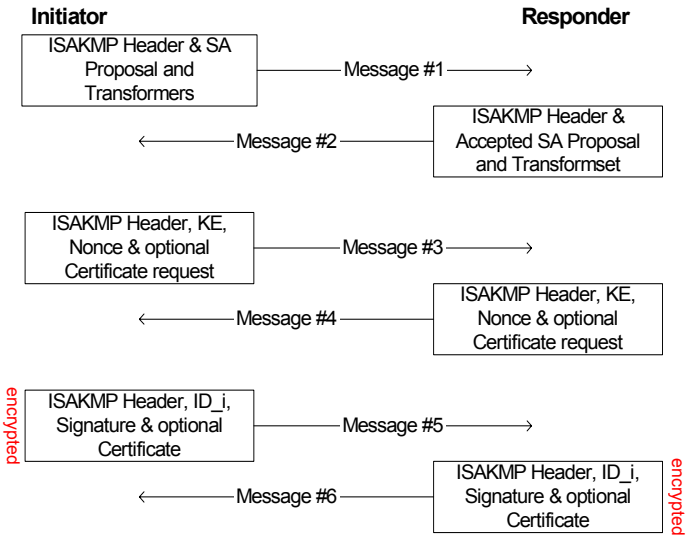
- Η Za ή SEG-to-SEG διασύνδεση (μεταξύ παρόχων).
- Η Zb ή SEG-to-NE και NE-to-NE διασύνδεση (εντός του δικτύου του παρόχου).

Το πρωτόκολλο IPsec (Frankel, 2001; Oppliger, 2002; Tiller, 2000) και το IKE (Kaufman, 2004; Maughan et al., 1998) ειδικότερα, αποτελούν μια πολύ ανταγωνιστική λύση. Όπως είδαμε, η 3GPP χρησιμοποιεί προ-εγκατεστημένα μυστικά κλειδιά (pre-shared secrets) για τη φάση I του IKE. Αυτό σημαίνει ότι κάθε NE πρέπει να διαμορφωθεί έτσι ώστε κάποιο συνθηματικό να αντιστοιχισθεί με κάθε IP διεύθυνση απομακρυσμένου (remote) συστήματος που

αυθεντικοποιείται από το NE. Ως αποτέλεσμα, τα κλειδιά που θα χρησιμοποιηθούν για κρυπτογράφηση και αυθεντικοποίηση (SKEYID_*), μετά την ολοκλήρωση της φάσης I του IKE, θα έχουν παραχθεί, λαμβάνοντας υπόψη μόνο τη συγκεκριμένη IP διεύθυνση.

Άρα, σε σενάρια που η IP διεύθυνση αποδίδεται με δυναμικό τρόπο, ο ερωτώμενος (responder) δεν μπορεί να διατηρήσει προ-εγκατεστημένα συνθηματικά, τα οποία αντιστοιχούν σε στατικές IP διευθύνσεις. Επιπλέον, το κύριο μειονέκτημα των προ-εγκατεστημένων μυστικών είναι η απουσία κάποιου ασφαλούς και κλιμακούμενου μηχανισμού για την ανταλλαγή τους. Κάτι τέτοιο είναι κατάλληλο μόνο σε μικρής κλίμακας δικτυακά περιβάλλοντα με περιορισμένο πλήθος NE. Ακόμη και σ' αυτή την περίπτωση, αν κάποιο μυστικό διαρρεύσει, δεν υπάρχει κάποια γενική μέθοδος ειδοποίησης του σχετικού NE και εκκίνησης της διαδικασίας αντικατάστασης (replacement).

Οι παραπάνω περιορισμοί μπορούν να ξεπεραστούν με επιτυχία, χρησιμοποιώντας εναλλακτικά λύσεις βασισμένες σε PKI (Kambourakis et al., 2003; Kambourakis et al., 2004; Kambourakis et al., 2004b). Έτσι, το πρωτόκολλο IKE μπορεί να εξασφαλίσει τη διαδικασία ανταλλαγής κλειδιών πάνω από τις Za & Zb διασυνδέσεις, ενώ η αυθεντικοποίηση μπορεί να βασιστεί σε ψηφιακές υπογραφές και PKC, αντί σε προ-εγκατεστημένα μυστικά. Η σειρά των μηνυμάτων που ανταλλάσσονται για την ολοκλήρωση της παραπάνω διαδικασίας παρουσιάζεται στο σχήμα 3-4.



Σχήμα 3-4. IKE Main mode με ψηφιακές Υπογραφές

Σ' αυτή την περίπτωση, τα κλειδιά κρυπτογράφησης και αυθεντικοποίησης των μηνυμάτων παράγονται με βάση τις ψευδό-τιμές (nonce) των NE και την τιμή Diffie-Hellman (SKEID=Pseudo_random_function(Nonce_i | Nonce_r , DH_Key). Η αυθεντικοποίηση των επικοινωνούντων NE μπορεί να επιτευχθεί με εκατέρωθεν αιτήσεις για ανταλλαγή ψηφιακών πιστοποιητικών. Το κάθε NE πρέπει να διαθέτει το δημόσιο κλειδί του άλλου για να είναι

δυνατή η επιβεβαίωση της ψηφιακής υπογραφής στην τρίτη ανταλλαγή (μηνύματα 5 & 6). Επιπλέον, η χρήση PKCs με βάση το συγκεκριμένο σενάριο μπορεί να παρέχει και υπηρεσίες μη-αποποίησης (για την ανταλλαγή των κλειδιών).

3.3.2. Το πρωτόκολλο SSL/TLS

Μια ακόμα λύση, η οποία πηγάζει από την εισαγωγή της τεχνολογίας PKI, είναι το γνωστό πρωτόκολλο Secure Sockets Layer (SSL) ή Transport Layer Security (TLS), το οποίο μπορεί να χρησιμοποιηθεί για την εξασφάλιση των επικοινωνιών μεταξύ των SEGs αλλά και των NEs. Είναι γνωστό ότι το πρωτόκολλο SSL/TLS, όταν συνδυάζεται με ψηφιακά πιστοποιητικά εξασφαλίζει αμοιβαία αυθεντικοποίηση των NEs. Είναι επίσης χαρακτηριστικό, ότι το SSL/TLS διαθέτει πολλά από τα πλεονεκτήματα του IPsec. Επιπλέον, η αποτελεσματικότητά του έχει αποδειχθεί πολλές φορές από την επιτυχημένη χρήση του στο ενσύρματο Διαδίκτυο. Το SSL/TLS μπορεί να αποτελέσει τμήμα ενός *all-IP* περιβάλλοντος κινητών επικοινωνιών, λαμβάνοντας υπόψη ότι εκτελείται πάνω από το TCP/IP και κάτω από τα επιπέδου εφαρμογής πρωτόκολλα, όπως το HTTP και το FTP και κατά συνέπεια η TCP επικεφαλίδα δεν είναι κρυπτογραφημένη.

Για παράδειγμα, η χρήση Performance Enhancing Proxies (PEPs) σε περιβάλλον 3G παράλληλα με IPsec, μπορεί να δημιουργήσει σημαντικό κενό στην ασφάλεια. Τα PEPs βελτιώνουν την απόδοση των ασύρματων TCP συνδέσεων μεταξύ των στοιχείων του δικτύου και των τελικών χρηστών. Συνήθως τα PEPs υλοποιούνται στο Radio Network Controller (RNC). Είναι λοιπόν σαφές ότι το PEP στοιχείο πρέπει να αποκρυπτογραφήσει την κρυπτογραφημένη IP επικεφαλίδα για να την επεξεργαστεί (Assaf et al., 2002). Έτσι, ή τα IP πακέτα πρέπει να αγνοήσουν την ύπαρξη PEP και έτσι να μην ωφεληθούν από την παρουσία του, ή ο τελικός χρήστης θα πρέπει να εμπιστευθεί το PEP στοιχείο (στη μέση). Βεβαίως, στη γενική περίπτωση, το τελικό σύστημα δεν μπορεί να εμπιστευτεί το PEP.

3.3.3. Το υποσύστημα πολυμέσων του UMTS (IM Subsystem)

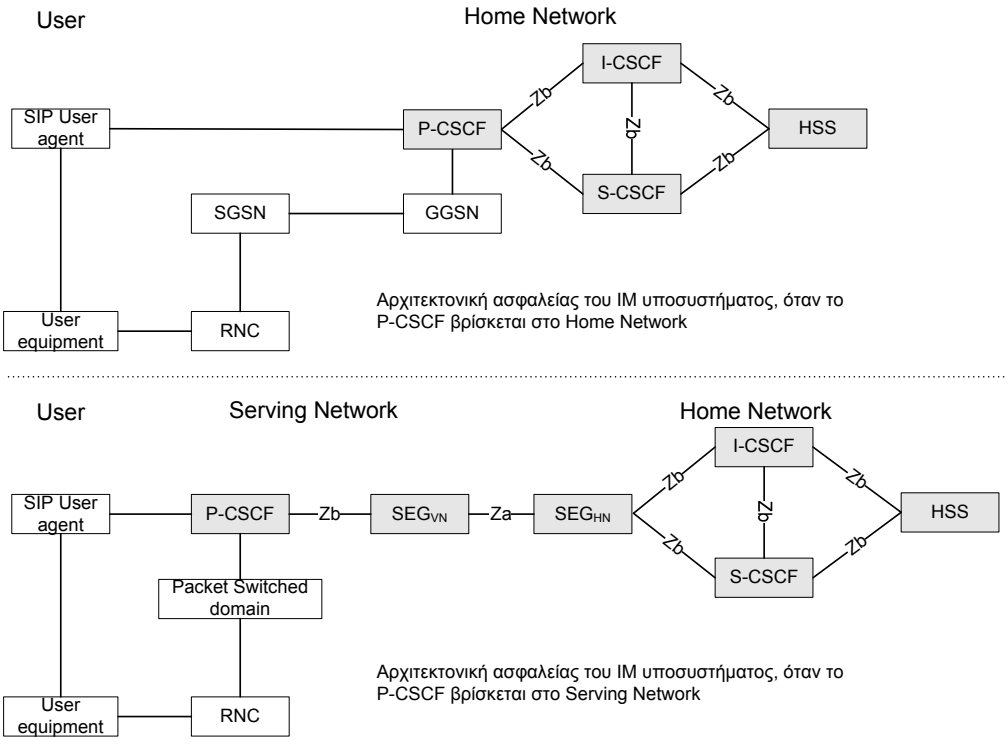
Η περίπτωση της application-level εγγραφής που εμφανίζεται στην έκδοση 6 του UMTS και παρουσιάζεται παρακάτω, αποδεικνύει ακόμη περισσότερο την ανάγκη ύπαρξης μηχανισμών δημόσιου κλειδιού. Σε ένα all-IP δίκτυο, το UE διεξάγει δύο διαφορετικούς τύπους εγγραφής (3GPP TS, 2002b; Lin et al., 2002):

Bearer-level εγγραφή και αυθεντικοποίηση: Όπου το UE εγγράφεται στο GPRS δίκτυο σύμφωνα με τις συνήθεις διαδικασίες σύνδεσης (attach) στο δίκτυο ή ανανέωσης της περιοχής δρομολόγησης (routing area update) (3GPP TS, 2002c). Κατά τη διάρκεια αυτής της διαδικασίας το UE αποκτά διεύθυνση IP και ανακαλύπτει, χρησιμοποιώντας την υπηρεσία DNS, τον τοπικό Proxy Call State Control Function (P-CSCF). Γενικά ένα CSCF αναπαριστά ένα SIP

εξυπηρέτη. Το SIP είναι ένα πρωτόκολλο εφαρμογής, βασισμένο σε μηνύματα κειμένου (text based), το οποίο εξυπηρετεί συνδέσεις τύπου πελάτη – εξυπηρέτη. Μπορεί να χρησιμοποιηθεί για τις ανάγκες σηματοδοσίας για την εγκαθίδρυση, μεταβολή και τερματισμό πολυμεσικών συνόδων των τελικών χρηστών. Έχει επιλεγεί από την 3GPP για την εξυπηρέτηση εφαρμογών πολυμέσων στα 3G δίκτυα. Όταν κάποιος χρήστης εγγράφεται σε ένα SIP εξυπηρέτη, λαμβάνει ένα μοναδικό SIP URL της μορφής *sip@username:domainname*. Ο χρήστης μπορεί να κινείται στο HN ή στο SN. Ο P-CSCF παρέχει βασική υποστήριξη για πολυμεσικές εφαρμογές και λειτουργεί και ως ανάχωμα ασφαλείας για το IP-Multimedia (IM) υποσύστημα.

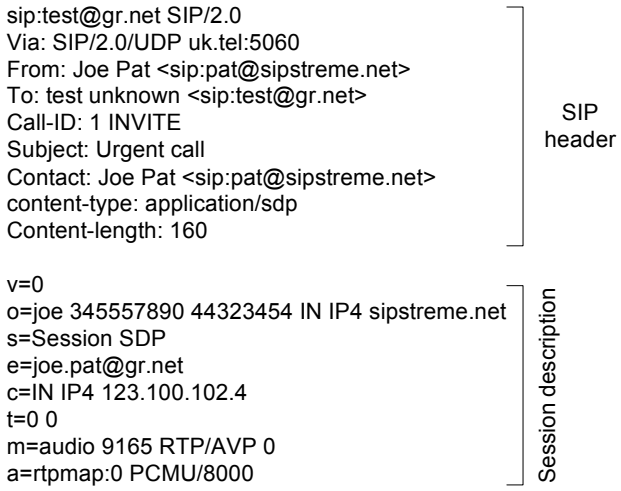
Application-level εγγραφή και αυθεντικοποίηση: Όπου ένα Serving CSCF (S-CSCF) ανατίθεται στο UE. Το τελευταίο αποστέλλει ένα μήνυμα REGISTER στο P-CSCF το οποίο αναμεταδίδεται (relay) ένα Interrogating-CSCF (I-CSCF) στο HN (το HN μπορεί να βρεθεί από το P-CSCF με βάση το IMSI ή το SIP URL του χρήστη). Έτσι το I-CSCF λειτουργεί ως μια πύλη (gateway) για το SN. Το I-CSCF στο HN επικοινωνεί με το HSS και ανακαλεί τα στοιχεία (IM profile) του χρήστη. Ακολούθως, επιλέγει ένα S-CSCF το οποίο θα προσφέρει στο χρήστη την απαιτούμενη υπηρεσία. Σημειώνεται, ότι τα S-CSCF έχουν πρόσβαση σε πόρους, όπως media gateways, video εξυπηρέτες κ.ά., για τη δημιουργία και τη διαχείριση τέτοιου είδους υπηρεσιών.

Παρατηρούμε, λοιπόν, ότι ένα πλήθος NE εμπλέκονται και συμμετέχουν στην application-level εγγραφή, ιδιαίτερα μάλιστα όταν το P-CSCF βρίσκεται στο SN (βλ. σχήμα 3-5).



Σχήμα 3-5. Αρχιτεκτονική ασφαλείας του IM υποσυστήματος (UMTS)

Επιπλέον, τα δεδομένα τα οποία μεταφέρονται έχουν ιδιαίτερη αξία και για το δίκτυο αλλά και για τους τελικούς χρήστες. Μεταξύ άλλων (για παράδειγμα, οι CSCF-UE παράμετροι που αποστέλλονται από το HSS στο I-CSCF), τα SIP μηνύματα μπορούν να περιέχουν εμπιστευτικές πληροφορίες που αφορούν τους χρήστες ή τους εξυπηρέτες. Για παράδειγμα, οι SIP επικεφαλίδες μπορεί να αποκαλύπτουν πληροφορίες για το ποιος επικοινωνεί με ποιον. Ομοίως, το κύριο τμήμα ενός SIP μηνύματος μπορεί να περιέχει εμπιστευτικές για τους χρήστες πληροφορίες (τύπος μέσου, διευθύνσεις, codec και πόρτες (ports) επικοινωνίας), οι οποίες είναι δυνατό να αποκαλυφθούν (βλ. σχήμα 3-6).

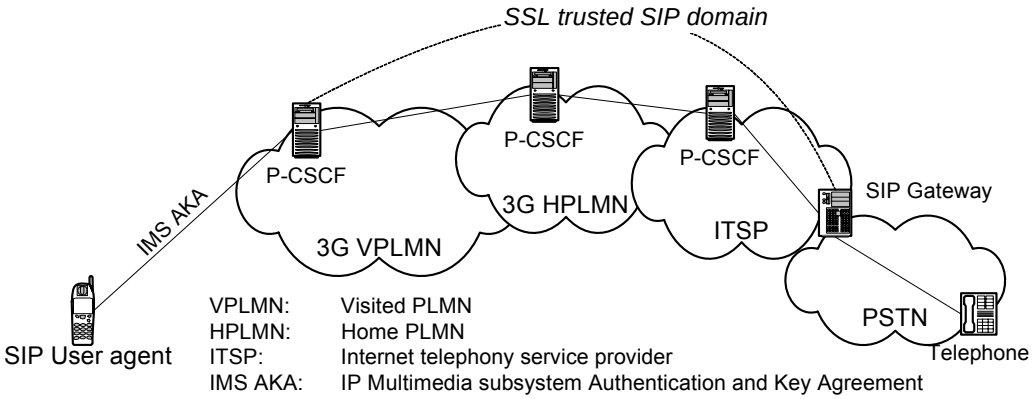


Σχήμα 3-6. Ένα τυπικό μήνυμα SIP

Οι διαδικασίες ασφάλειας θα πρέπει να προστατεύουν την εμπιστευτικότητα των δεδομένων του δικτύου και των χρηστών, αποτρέποντας επιθέσεις που έχουν ως στόχο τη μεταβολή ή τη δημιουργία SIP συνεδριών από μη-εξουσιοδοτημένους χρήστες (Salsano et al., 2002). Έτσι, ενώ η προστασία της εμπιστευτικότητας και της ακεραιότητας της SIP σηματοδοσίας, προσφέρεται με τρόπο από σημείο-σε-σημείο (*hop-by-hop*) και το ίδιο το SIP δεν ενσωματώνει (build-in) κάποιους μηχανισμούς ασφαλείας, αυτοί πρέπει να προσφερθούν από το δίκτυο (IPsec, SSL). Σημειώνεται, ότι οι μηχανισμοί από σημείο-σε-σημείο είναι απαραίτητοι εξαιτίας του ότι τα ενδιάμεσα NE μπορεί να εκτελούν κάποιο είδος επεξεργασίας, διαβάζοντας από ή γράφοντας σε συγκεκριμένα τμήματα των SIP μηνυμάτων.

Η 3GPP χρησιμοποιεί το πρωτόκολλο IPsec για την προστασία των επικοινωνιών μεταξύ των SIP οντοτήτων, οι οποίες έχουν προκαθορισμένες και αρκετά στατικές σχέσεις και πολιτικές ασφαλείας. Από την άλλη πλευρά, θεωρήστε ένα κινούμενο χρήστη, ο οποίος επιθυμεί να συνδεθεί σε ένα P-CSCF, το οποίο βρίσκεται στο δίκτυο ενός παρόχου υπηρεσιών διαδικτύου μέσω τηλεφώνου (Internet Telephony Service Provider, ITSP). Κανένας δεν μπορεί να εγγυηθεί ότι τα SIP δεδομένα θα μεταφερθούν με ασφάλεια απ' άκρο σ' άκρο, μέχρι ο χρήστης να λάβει την τελική υπηρεσία.

Είναι χαρακτηριστικό ότι η τελευταία έκδοση του SIP (Rosenberg et al., 2002), περιλαμβάνει διαδικασίες βασισμένες στο πρωτόκολλο SSL, με τις οποίες μπορεί κάποιο NE (π.χ. χρήστης ή εξυπηρέτης) να προσπελαστεί με ασφάλεια (βλ. σχήμα 3-7). Σ' αυτή την περίπτωση, ένας νέος τύπος SIP URI έχει οριστεί, για παράδειγμα *sips:test@secure.com*, ο οποίος υποδεικνύει τη χρήση SSL. Αυτή η προσέγγιση είναι ιδιαίτερα βολική σε αρχιτεκτονικές στις οποίες απαιτείται *hop-by-hop* ασφάλεια με χρήση δυναμικών και εύκαμπτων συσχετισμών ασφαλείας (SAs), που χρησιμοποιούν μεθόδους δημόσιου κλειδιού.



Σχήμα 3-7. SIP κλήση εξασφαλισμένη με SSL μεταξύ διαφορετικών δικτύων

3.4. Σύνοψη – Συμπεράσματα

Το ολοένα αυξανόμενο πλήθος των χρηστών υπηρεσιών κινητών επικοινωνιών αναμένει από τους αντίστοιχους παρόχους να προσφέρουν υψηλή ποιότητα και διαθεσιμότητα υπηρεσιών. Γι' αυτό το λόγο, νέοι, περισσότερο ευέλικτοι και ευπροσαρμόσιμοι μηχανισμοί ασφαλείας είναι αναγκαίοι προκειμένου να υποστηρίξουν την αναμενόμενη *all-IP* αρχιτεκτονική στα πλαίσια του 4G μοντέλου.

Προς το παρόν η 3GPP βασίζεται σε λύσεις ασφαλείας που μπορεί να προσφέρει το συμμετρικό μοντέλο για να καλύψει τις ανάγκες για δια-δικτυακή και ενδο-δικτυακή προστασία των κεντρικών δικτύων των παρόχων. Αυτές οι επιλογές μπορεί να ικανοποιούν τις ανάγκες των 2.5 προς 3G δικτύων, αλλά εκτιμάται ότι θα αποδειχθούν ανεπαρκείς στο μέλλον. Η αναμενόμενη ενοποίηση των ετερογενών δικτύων των παρόχων και του Διαδικτύου, δημιουργεί ένα ανοικτό δικτυακό περιβάλλον ευάλωτο σε επιθέσεις. Η ενσωμάτωση τεχνολογίας PKI είναι δυνατό να προσφέρει ισχυρές, κλιμακούμενες αλλά και δοκιμασμένες λύσεις ασφαλείας, οι οποίες μπορούν να αντεπεξέλθουν στις νέες αυτές συνθήκες.

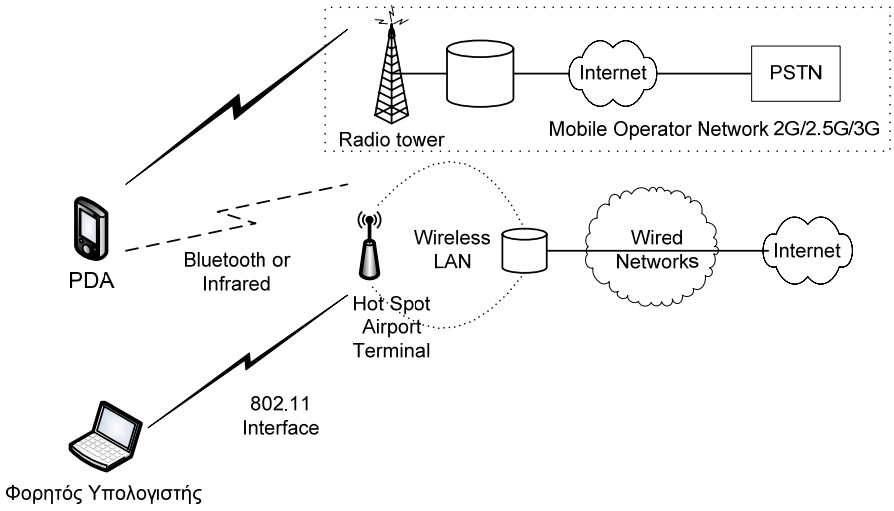
Κεφάλαιο 4: Αυθεντικοποίηση χρηστών 3G και B3G με χρήση πρωτοκόλλων δημόσιου κλειδιού και υποστήριξη PKI.

4.1. Εισαγωγή

Σύμφωνα με τη B3G προοπτική, ο κορμός των κεντρικών δικτύων όλων των ετερογενών ασύρματων τεχνολογιών θα βασίζεται στο πρωτόκολλο IP, ενώ η παροχή υψηλής ποιότητας υπηρεσιών ασφαλείας αποτελεί έναν από τους βασικούς στόχους αυτών των συστημάτων. Όπως αναφέρθηκε στο Κεφάλαιο 3, το πρωτόκολλο SSL/TLS (Frier et al., 1996; Dierks and Allen, 1999; Rescorla, 2001; Boyd & Mathuria, 2003) αποτελεί ίσως το σημαντικότερο και περισσότερο χρησιμοποιούμενο πρωτόκολλο ασφαλείας στο ενσύρματο Διαδίκτυο. Παρόλα αυτά, μέχρι σήμερα, καμιά ασύρματη υπηρεσία δεν προσφέρει το πρωτόκολλο αυτό σε κινητή συσκευή.

Λόγοι επιδόσεων (performance) σε περιβάλλον περιορισμένων υπολογιστικών και αποθηκευτικών πόρων (resources), όπως είναι οι κινητές συσκευές, οδήγησαν τους κατασκευαστές να σχεδιάσουν ένα διαφορετικό, ασύμβατο (incompatible) και βασισμένο σε πύλες (gateway oriented) πρωτόκολλο ασφαλείας, το οποίο ονομάστηκε Wireless Transport Layer Security (WTLS) (WAP Forum, 2001; Khare, 1999).

Υπό την προϋπόθεση ότι είναι δυνατό να αναπτύξουμε μια αποδοτική, με όρους επιδόσεων υλικού (hardware) φορητή συσκευή (handheld device), όπως αναπτύσσεται στο (Gupta, 2002), μπορούμε να θεωρήσουμε τη διαδικασία αυθεντικοποίησης μεταξύ των χρηστών κινητών επικοινωνιών και των παρόχων των υπηρεσιών αυτών ως υπηρεσία, η οποία θα εκτελείται σε υψηλότερο επίπεδο (κάτω από το επίπεδο εφαρμογής). Ως αποτέλεσμα, μπορούμε να υλοποιήσουμε περισσότερο ασφαλείς, ευέλικτες, ευπροσαρμόσιμες και ανεξάρτητες της τεχνολογίας πρόσβασης δικτύου διαδικασίες αυθεντικοποίησης και συμφωνίας κλειδιού (Authentication and Key Agreement, AKA) για τα 3G και 4G συστήματα κινητών επικοινωνιών (Kambourakis et al., 2002; Dixit & Prasad, 2004; Wisely et al., 2002). Στο σχήμα 4-1 παρουσιάζεται μια άποψη 4G περιβάλλοντος.



Σχήμα 4-1. Περιβάλλον 4G

Το παρόν κεφάλαιο προτείνει ένα μηχανισμό AKA βασισμένο σε SSL, λαμβάνοντας υπόψη την απαραίτητη ενσωμάτωση PKI τεχνολογίας στα δίκτυα 3G και B3G. Επιπλέον, το προτεινόμενο σχήμα αξιολογείται (evaluate) με όρους αποδοτικότητας (χρόνοι, κατανάλωση μπαταρίας), χρησιμοποιώντας διαφορετικές διατάξεις. Τα αποτελέσματα των μετρήσεων δείχνουν ότι μια διαδικασία αυθεντικοποίησης βασισμένη στο πρωτόκολλο SSL μπορεί να αποτελέσει μια εφικτή και αξιόπιστη επιλογή για τα μελλοντικά συστήματα κινητών επικοινωνιών.

4.2. SSL και PKI σε περιβάλλον κινητών Επικοινωνιών

Το πρωτόκολλο SSL/TLS εγκαθιδρύει έναν ασφαλή δίαυλο επικοινωνιών στο επίπεδο μεταφοράς. Το SSL διαθέτει πολλά πλεονεκτήματα, όπως υποστήριξη για διαφορετικές εφαρμογές, απαίτηση για ελάχιστες τροποποιήσεις στα επίπεδα πάνω και κάτω απ' αυτό και εύκολη υλοποίηση σε IP συσκευές. Η επιτυχημένη χρήση του SSL στο ενσύρματο Διαδίκτυο εδώ και πολλά χρόνια έχει αποδείξει την αποτελεσματικότητά και χρησιμότητά του. Όλοι σχεδόν οι WEB εξυπηρέτες υποστηρίζουν κάποια έκδοσή του. Ομοίως, το SSL μπορεί να αποτελέσει τμήμα ενός *all-IP* περιβάλλοντος κινητών επικοινωνιών (Gupta, 2002).

Επιπλέον, το SSL υποστηρίζει αρκετά πρωτόκολλα για τη δημιουργία pre-master κλειδιών (RSA, Diffie-Hellman, κ.ά.) και διαφορετικούς αλγορίθμους κρυπτογράφησης και προστασίας της ακεραιότητας και αυθεντικότητας (Message Authentication Code, MAC) των δεδομένων. Στα πλαίσια ενός AKA μηχανισμού, που χρησιμοποιείται σε ένα διαρκώς εξελισσόμενο περιβάλλον, οι παραπάνω ιδιότητες μπορούν να προσδώσουν σημαντική ευελιξία. Επίσης, όπως θα δούμε παρακάτω, η ενσωμάτωση των λειτουργιών εκπομπής του IMSI και της ανάθεσης προσωρινής ταυτότητας συνδρομητή (Packet-Temporary Mobile Subscriber Identity,

P-TMSI) στο μηχανισμό SSL AKA προσφέρει αυξημένη αξιοπιστία και λιγότερες ευκαιρίες στους επιτιθέμενους (attackers).

Τα τελευταία χρόνια, οι έξυπνες κάρτες (smart cards) ενσωματώνουν όλο και πιο προηγμένες αρχιτεκτονικές. Έτσι, είναι σε θέση να αποθηκεύουν με ασφαλή τρόπο τα ιδιωτικά κλειδιά των συνδρομητών, να λειτουργούν αποτελεσματικά ως γεννήτριες ψευδο-τυχαίων αριθμών και να αναλαμβάνουν διαδικασίες ενθυλάκωσης και απενθυλάκωσης για την ασφαλή μεταφορά συμμετρικών κλειδιών (Gupta, 2002; Nash et al., 2001). Για παράδειγμα, η κάρτα Schlumberger Cyberflex μπορεί να εκτελέσει RSA λειτουργίες των 1024 bits, σε λιγότερο από ένα δευτερόλεπτο. Οι σύγχρονες κινητές συσκευές επικοινωνιών διαθέτουν αρκετούς πόρους (γρήγορους επεξεργαστές και μνήμη) για να αντεπεξέλθουν στις απαιτήσεις του ίδιου του πρωτοκόλλου.

Η ερευνητική δραστηριότητα ASPeCT (ASPeCT, 1999) απέδειξε ότι είναι δυνατό να υλοποιηθούν αποτελεσματικοί μηχανισμοί αυθεντικοποίησης με χρήση δημόσιων κλειδιών για τα συστήματα GSM και UMTS. Επίσης, μια πρόσφατη μελέτη έδειξε ότι το πρωτόκολλο SSL είναι δυνατό να χρησιμοποιηθεί αποτελεσματικά σε κινητές συσκευές επικοινωνιών (Gupta, 2002). Διάφορα ερευνητικά άρθρα διερευνούν την πιθανότητα χρήσης SSL σε περιβάλλον κινητών επικοινωνιών με proxy αρχιτεκτονικές (Burnside et al., 2002), ενώ σχετικές εργασίες έδειξαν ότι το πρωτόκολλο χειραψίας (SSL handshake protocol) μπορεί να βελτιωθεί έως και 5.7 φορές (Potlapally et al., 2002).

Όπως είναι φυσικό, προκειμένου να σχεδιάσουμε μια διαδικασία AKA, η οποία θα βασίζεται σε SSL, θα πρέπει να χρησιμοποιήσουμε (π.χ. για την παροχή ψηφιακών πιστοποιητικών) στοιχεία PKI. Εκτός από τις απαιτήσεις που αναπτύχθηκαν στις ενότητες 2.3.1 & 3.2.3 αναφέρουμε τα εξής:

- Εφόσον το IMSI κάθε συνδρομητή μπορεί να αποκαλύψει την πραγματική του ταυτότητα, αυτό πρέπει να αποθηκεύεται με ασφαλή τρόπο στη UICC κάρτα του μαζί με το ιδιωτικό του κλειδί και τα δημόσια κλειδιά όλων των έμπιστων CAs.
- Η UICC κάρτα θα πρέπει να μπορεί να δημιουργεί ασφαλείς ψευδοτυχαίες τιμές και να εκτελεί λειτουργίες με δημόσια κλειδιά. Για παράδειγμα, αν πρόκειται να χρησιμοποιηθεί RSA για τη δημιουργία pre-master μυστικού (όπως στο MS key exchange μήνυμα βλ. ενότητα 4.3.2), η UICC δημιουργεί μια τιμή pre-master μυστικού μήκους 48 bytes και την κρυπτογραφεί (ενθυλακώνει), χρησιμοποιώντας το δημόσιο RSA κλειδί του εξυπηρέτη. Αυτό σημαίνει ότι το UE πρέπει να «περάσει» το δημόσιο κλειδί του εξυπηρέτη στην UICC. Το UE πρέπει επίσης να μπορεί να διεκπεραιώνει με ταχύτητα τους υπόλοιπους υπολογισμούς που προβλέπονται από το πρωτόκολλο. Επιπλέον, το UE πρέπει να διαθέτει ποσότητα μη-μεταβλητής μνήμης (non-volatile) για την αποθήκευση του P-TMSI και

των SSL παραμέτρων για την υποστήριξη συνόδων με επανάληψη (SSL session resumption), όπως περιγράφεται στην ενότητα 4.3.3.

- Ο μηχανισμός AKA παρέχεται από τα SGSNs, SIP εξυπηρέτες (CSCF) και από τους 3GPP Authentication Authorization Accounting (AAA) εξυπηρέτες.

4.3. AKA μηχανισμός βασισμένος στο SSL πρωτόκολλο

4.3.1. Περιορισμοί και Προβλήματα του Μηχανισμού 3GPP AKA

Στο UMTS ο μηχανισμός AKA είναι σχεδιασμένος στα πρότυπα του αντίστοιχου μηχανισμού του GSM. Η διαδικασία αυθεντικοποίησης βασίζεται σε ένα συμμετρικό κλειδί *K,* το οποίο είναι αποθηκευμένο στη UICC κάρτα του συνδρομητή και στο αντίστοιχο HSS του HN. Η διαδικασία, όπως περιγράφεται στα (3GPP TS, 2002c; Niemi & Nyberg, 2004), βασίζεται στο πρωτόκολλο πρόκλησης – απάντησης (challenge – response). Επίσης, μια ολοκληρωμένη ανάλυση σχετικά με τις ομοιότητες και διαφορές στους μηχανισμούς ασφαλείας πρόσβασης στο δίκτυο (access security) μεταξύ των συστημάτων UMTS και CDMA2000, περιέχεται στο (Rose et al., 2004).

Αρκετά γνωστά προβλήματα και αδυναμίες του GSM AKA φαίνεται ότι έχουν λυθεί ή επαρκώς καλυφθεί στο UMTS AKA. Παρόλα αυτά, υπάρχουν ακόμη ορισμένα κενά ασφαλείας ή αδυναμίες, τις οποίες οι τυχόν επιτιθέμενοι (attackers) μπορούν να εκμεταλλευτούν. Οι αδυναμίες αυτές περιγράφονται σε συντομία στα παρακάτω, ενώ μια πιο λεπτομερής ανάλυση παρέχεται στα (3GPP TS, 2002c; 3GPP TS, 2000; Aamodt et al., 2001; Niemi & Nyberg, 2004).

1. 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. Το πρόβλημα απαιτεί ιδιαίτερη προσοχή στην περίπτωση που ένας συνδρομητής περιάγει (roams) μεταξύ διαφορετικών PLMNs. Τότε το HN είναι υποχρεωμένο να αποστείλει στο SN διανύσματα αυθεντικοποίησης προκειμένου το τελευταίο να μπορεί να αυθεντικοποιήσει το συνδρομητή. Σε τέτοιες περιπτώσεις τα διανύσματα μεταφέρονται μεταξύ των διαφορετικών δικτύων των παρόχων (οι οποίοι μπορεί να εφαρμόζουν διάφορες πολιτικές ασφαλείας) και έτσι είναι περισσότερο πιθανό να υποκλαπούν ή να καταστραφούν. Σε κάθε περίπτωση, όπως συνέβαινε και στο GSM, οι χρήστες πρέπει να εμπιστεύονται το SN και τις πολιτικές ασφάλειας που αυτό εφαρμόζει.

2. Σε ορισμένες περιπτώσεις, το σύστημα επιτρέπει την εκπομπή του IMSI του χρήστη από το UE στο δίκτυο σε μορφή καθαρού κειμένου (clear-text) με σκοπό αυτός να αυθεντικο-

ποιηθεί. Η συγκεκριμένη διαδικασία μπορεί να εκκινηθεί από το HN ή το SN στις ακόλουθες περιπτώσεις: (α) Όταν ο συνδρομητής εγγράφεται για πρώτη φορά στο δίκτυο ή μετά από μεγάλο διάστημα κατά το οποίο διατηρούσε τη συσκευή του εκτός λειτουργίας και (β) Όταν το δίκτυο δεν μπορεί να ανακτήσει το IMSI του συνδρομητή. Όπως για παράδειγμα, σε περιπτώσεις μεταβίβασης κλήσης ή συνεδρίας (session) από κυψέλη σε κυψέλη ή από δίκτυο σε δίκτυο (handover), όπου το ζευγάρι IMSI, P-TMSI μεταδίδεται από το προηγούμενο SGSN στο νέο και η IP διεύθυνση του προηγουμένου SGSN δεν μπορεί να επιλυθεί (resolved). Επίσης, σε περιπτώσεις κατά τις οποίες η βάση δεδομένων ενός SGSN παρουσιάζει βλάβη. Η διαδικασία αυτή είναι ανοικτή σε παθητικού τύπου επιθέσεις, όπου ο επιτιθέμενος περιμένει για πιθανές εκπομπές απροστάτευτων IMSI ή σε επιθέσεις τύπου MITM (3GPP TS, 2000). Η εκπομπή του IMSI αποτελεί κυρίως απειλή εναντίον της εμπιστευτικότητας της ταυτότητας του χρήστη (identity confidentiality) και της θέσης που αυτός κινείται (location privacy). Επιπλέον, όμως, η γνώση του IMSI μπορεί να επιτρέψει την πλαστογράφηση της ταυτότητας του χρήστη. Δεν είναι βέβαια σαφές το πώς ένας επιτιθέμενος μπορεί να εκμεταλλευτεί αυτή τη δυνατότητα πλαστογράφησης, πέραν του να προκαλέσει γενική αναστάτωση (commotion) στο σύστημα.

3. Το μήκος των κλειδιών και οι αλγόριθμοι κρυπτογράφησης / αποκρυπτογράφησης είναι σταθερά (fixed), με αποτέλεσμα ο μηχανισμός AKA να θεωρείται δύσκαμπτος (inflexible) και λιγότερο ασφαλής. Αυτό είναι ιδιαίτερα εμφανές σε περιπτώσεις όπου ανακαλύπτεται μια ευπάθεια (vulnerability) σε κάποιον αλγόριθμο ή διαδικασία, όπως στην περίπτωση του αλγορίθμου GSM A5/1 (Biryukov & Shamir, 1999). Αντίθετα, μεγαλύτερη ευελιξία επιτυγχάνεται έχοντας ένα δυναμικό μηχανισμό AKA, ο οποίος είναι ικανός να διαπραγματεύεται και να ενσωματώνει νέα στοιχεία (modules) ασφαλείας σε πραγματικό χρόνο και ανάλογα με τις συνθήκες (on-demand).

4. Μία από τις βελτιώσεις ασφαλείας στο UMTS είναι η συμπερίληψη της δυνατότητας προστασίας της ακεραιότητας. Όμως, η προστασία της ακεραιότητας είναι εγγυημένη μόνο για τη σηματοδοσία μεταξύ UE και RNC. Στα δεδομένα των χρηστών δεν προσαρτάται MAC και γι' αυτό το λόγο παραμένουν ευαίσθητα σε παραποιήσεις (manipulation).

5. Οι μηχανισμοί αυθεντικοποίησης και δημιουργίας κλειδιών θα πρέπει, πέραν της προστασίας της επικοινωνίας, να προσφέρουν υπηρεσίες ασφαλείας για πολυμεσικές εφαρμογές και IP υπηρεσίες. Η πρόκληση είναι ακόμα μεγαλύτερη, όταν το ασύρματο περιβάλλον αποτελείται από πολλαπλούς, ετερογενείς και αυτό-ρυθμιζόμενους (self-configuring) τομείς (domains).

Επίσης, προστασία στο επίπεδο εφαρμογής, όπου αυτή απαιτείται, παρέχεται από το πρωτόκολλο WTLS. Είναι γνωστό πως το WTLS, τουλάχιστον μέχρι την έκδοση 2.0, χρησιμοποιεί

WAP πύλη (gateway), η οποία θεωρείται γενικά ανασφαλής και σίγουρα δεν εξασφαλίζει end-to-end επικοινωνία. Επιπλέον, επιτρέπει τη χρησιμοποίηση «αδύνατων» (weak) αλγορίθμων κρυπτογράφησης και διαθέτει χαρακτηριστικά, τα οποία επιτρέπουν την ανάπτυξη επιθέσεων του τύπου επιλεγμένου κειμένου (chosen-plaintext) και εξαντλητικής αναζήτησης (brute force). Σε κάθε περίπτωση, η διαδικασία αυθεντικοποίησης του WTLS είναι συχνά ανώνυμη, ενώ ακόμη και όταν αυτή εκτελείται κανονικά, γίνεται μόνο μια φορά (έναντι της WAP πύλης) σε όλη τη διάρκεια χρησιμοποίησης της πύλης.

4.3.2. Περιγραφή του μηχανισμού AKA SSL

Όπως αναφέρθηκε στα παραπάνω, ο 3GPP AKA μηχανισμός βασίζεται σε ένα συμμετρικό κλειδί *K,* το οποίο χρησιμοποιείται από τις μονόδρομες (one-way) συναρτήσεις *f1* έως *f5* για τον υπολογισμό και την επαλήθευση των διανυσμάτων αυθεντικοποίησης. Οι συναρτήσεις *f1* και *f2* είναι συναρτήσεις αυθεντικοποίησης μηνύματος, ενώ οι *f3*, *f4* και *f5* χρησιμοποιούνται για την παραγωγή του κλειδιού κρυπτογράφησης – αποκρυπτογράφησης. Η λειτουργία των παραπάνω συναρτήσεων περιγράφεται αναλυτικά στα (3GPP TS, 2002c; Koien, 2004; Niemi & Nyberg, 2004). Η διαδικασία αυθεντικοποίησης είναι αμοιβαία, δηλαδή η εφαρμογή USIM αυθεντικοποιείται στο δίκτυο και το δίκτυο στη USIM. Όπως αναπτύχθηκε στην προηγούμενη ενότητα, υπάρχει πάντοτε η πιθανότητα για έναν επιτιθέμενο να υποκλέψει διανύσματα αυθεντικοποίησης. Αν αυτά δεν έχουν ήδη χρησιμοποιηθεί, τότε είναι πιθανό ο τελευταίος να επιτύχει τους σκοπούς του, προσποιούμενος είτε το δίκτυο (false base station attack) είτε το χρήστη (false UE attack).

Με αφορμή τις τελευταίες τεχνολογικές τάσεις, οι οποίες αναφέρθηκαν στην ενότητα 4.2, προτείνουμε ένα μηχανισμό AKA, που βασίζεται στο πρωτόκολλο SSL, μπορεί να χρησιμοποιηθεί στο PS υποσύστημα και περιλαμβάνει διαδικασία ανάθεσης P-TMSI και απόκρυψης – προστασίας του IMSI από ενεργητικού ή παθητικού τύπου υποκλοπές (Kambourakis et al., 2004c; Kambourakis et al., 2004d). Η ροή και οι ανταλλαγές μηνυμάτων μεταξύ UE, SGSN και HSS, κατά τη διαδικασία αυθεντικοποίησης παρουσιάζονται στο σχήμα 4-2. Ο προτεινόμενος μηχανισμός μπορεί να υλοποιηθεί μελλοντικά ή σε dual-mode AKA συσκευές.

Ο μηχανισμός υποστηρίζει αμοιβαία αυθεντικοποίηση USIM – δικτύου μέσω X.509 PKCs. Τα συμμετρικά κλειδιά, τα οποία δημιουργούνται μετά το τέλος του πρωτοκόλλου χειραψίας, χρησιμοποιούνται για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων των χρηστών αλλά και της σηματοδοσίας. Προς το παρόν υποθέτουμε ότι στο μήνυμα αίτησης σύνδεσης με το δίκτυο (attach request), που αποστέλλεται από το UE στο SGSN, δεν περιλαμβάνεται κάποιο P-TMSI. Στις επόμενες ενότητες θα δείξουμε πως η διαδικασία μπορεί να επεκταθεί, όταν το συγκεκριμένο μήνυμα περιέχει και το P-TMSI του UE.

i. Η διαδικασία χειραψίας αρχικοποιείται από το UE, το οποίο αποστέλλει ένα μήνυμα *UE Hello* στο SGSN. Στο μήνυμα αυτό περιλαμβάνονται τα χαρακτηριστικά ασφαλείας που υποστηρίζει το UE: η υψηλότερη έκδοση του SSL πρωτοκόλλου, μια ταξινομημένη κατά προτίμηση λίστα των αλγορίθμων κρυπτογράφησης και συμπίεσης, μια 32-bit χρονοσφραγίδα (timestamp), μια 28-bit τυχαία αριθμητική τιμή και ένα αναγνωριστικό συνόδου (Session ID). Το τελευταίο πρέπει να είναι κενό (null), όταν το UE δε σκοπεύει να συνεχίσει μια προηγούμενη σύνοδο (βλ. ενότητα 4.3.3) και ζητάει από το SGSN τη δημιουργία μιας νέας.

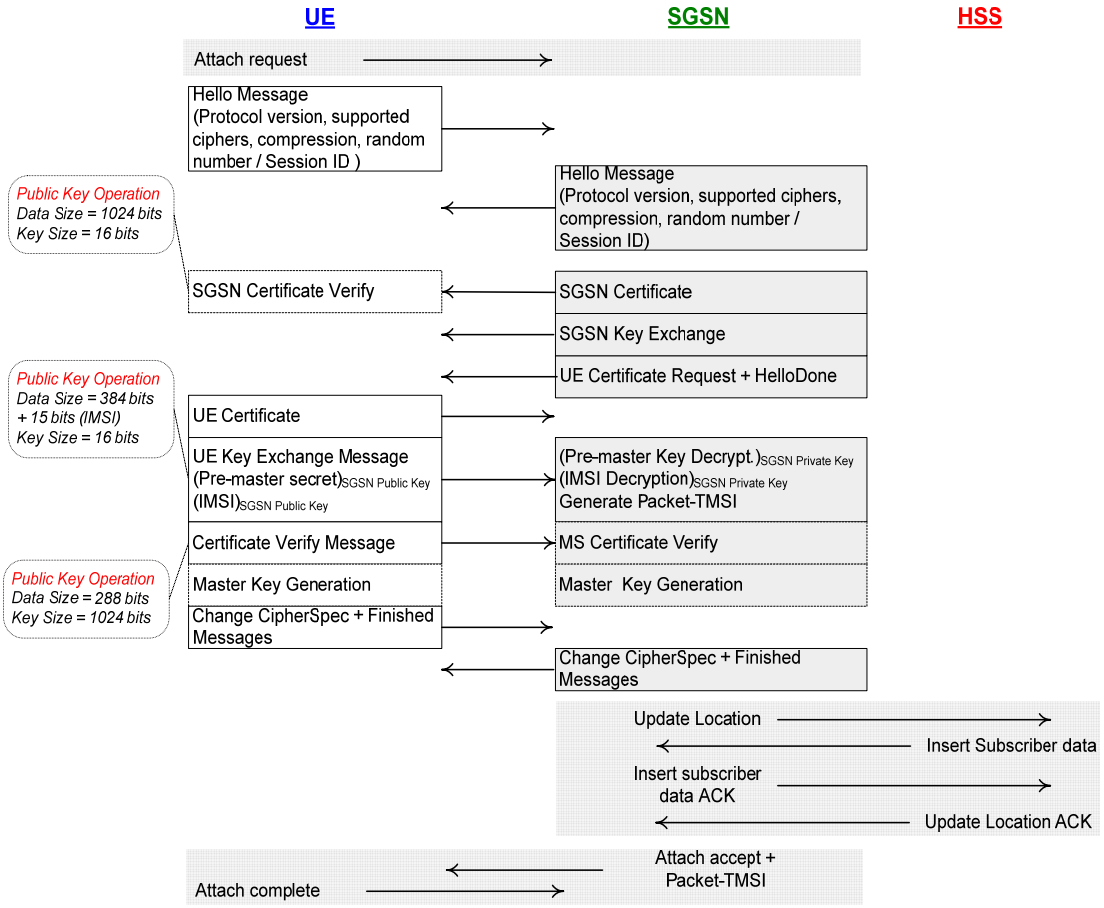
ii. Το SGSN απαντάει με το δικό του *Hello* μήνυμα. Αν υποστηρίζει κάποια κοινά χαρακτηριστικά ασφαλείας με το UE (αλγόριθμοι κρυπτογράφησης, κτλ) αυτά περιλαμβάνονται στο μήνυμα. Διαφορετικά η σύνδεση απορρίπτεται. Επιπλέον, το SGSN αποστέλλει τις δικές του 32-bit και 28-bit τιμές και ένα Session ID. Αν το τελευταίο είναι ίδιο με το αναγνωριστικό συνόδου του UE, τότε τα δύο μέρη συμφωνούν να επαναλάβουν μια προηγούμενη σύνοδο (που διακρίνονταν απ' αυτό το ID). Σε διαφορετική περίπτωση το SGSN δημιουργεί ένα νέο αναγνωριστικό συνόδου, υποδηλώνοντας μια νέα σύνδεση.

iii. Το SGSN αποστέλλει το ψηφιακό του πιστοποιητικό στο UE. Αυτό μπορεί να είναι της μορφής X.503v3 ή υποσύνολό του.

iv. Το SGSN αποστέλλει ένα μήνυμα ανταλλαγής κλειδιών (key-exchange) στο UE. Το βήμα αυτό είναι απαραίτητο προκειμένου να επιτραπεί στο UE να εξακριβώσει ότι πράγματι το SGSN έχει στην κατοχή του το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί, το οποίο περιέχεται στο πιστοποιητικό που στάλθηκε στο UE.

v. Το UE πρέπει να επαληθεύσει το πιστοποιητικό του SGSN. Πρώτα απ' όλα ελέγχει ότι το PKC έχει εκδοθεί από μια έμπιστη CA και η χρονική περίοδος ισχύος του δεν έχει λήξει (expired). Δεδομένου ότι οι μεταβολές στις λίστες με τις έμπιστες CAs είναι σπάνιες, μια τέτοια λίστα μαζί με τα αντίστοιχα δημόσια κλειδιά των CAs μπορεί να είναι αποθηκευμένη στην UICC. Είναι πολύ σημαντικό η διαδικασία επαλήθευσης του PKC της CA να χρησιμοποιεί το δημόσιο κλειδί που είναι αποθηκευμένο στην UICC, αντί αυτού που περιλαμβάνεται στην αλυσίδα (chain) PKC που έστειλε το SGSN. Το UE υπολογίζει μια σύνοψη (hash) του πιστοποιητικού του SGSN και τη συγκρίνει με αυτή που υπάρχει στο ίδιο το πιστοποιητικό, επαληθεύοντας την ψηφιακή υπογραφή του. Επίσης, δεν υπάρχει πραγματική ανάγκη για το UE να ελέγξει αν το PKC του SGSN έχει ανακληθεί. Το πλήθος των SGSN ή των εξυπηρετών αυθεντικοποίησης στη γενική περίπτωση, που διαχειρίζεται ένας πάροχος, είναι σχετικά μικρό (τάξη δεκάδων) ανάλογα με το συνολικό μέγεθος του δικτύου. Θεωρώντας ότι το δίκτυο κάθε παρόχου είναι σχε-

τικά κλειστό και ότι το ιδιωτικό κλειδί κάθε SGSN είναι επαρκώς προστατευμένο υ-πάρχουν οι παρακάτω επιλογές: (α) κάθε πάροχος μπορεί περιοδικά, για παράδειγμα κάθε 12-18 μήνες, να ανανεώνει τα πιστοποιητικά των SGSNs, ανακαλώντας τα παλιά και εκδίδοντας νέα. (β) Τα PKC των SGSNs μπορεί να έχουν περιορισμένη διάρκεια ζωής 12-18 μήνες. Πριν από τη λήξη τους θα πρέπει να αντικατασταθούν από τον πά-ροχο. (γ) Η τρίτη λύση προβλέπει ότι το πιστοποιητικό ενός SGSN αντικαθίσταται μόνο σε περίπτωση αναβάθμισης, διακοπής ή παύσης της λειτουργίας του.



Σχήμα 4-2. Μηχανισμός AKA βασισμένος σε SSL (Το P-TMSI είναι άγνωστο στο SGSN)

vi. Το SGSN ζητάει το πιστοποιητικό του UE και ολοκληρώνει τη συμμετοχή του στη δια-δικασία διαπραγμάτευσης με ένα μήνυμα *Hello Done*.

vii. Το UE / USIM παράγει μια *pre-master* τιμή και την κρυπτογραφεί, χρησιμοποιώντας το δημόσιο κλειδί του SGSN. Με παρόμοιο τρόπο κρυπτογραφεί και το IMSI του. Κατό-πιν, αποστέλλει και τις δύο τιμές στο SGSN. Αν η ανταλλαγή κλειδιών βασίζεται στο πρωτόκολλο Diffie-Hellman, τότε τα δύο μέρη ανταλλάσσουν τις δημόσιες παραμέ-τρους τους, χρησιμοποιώντας τα μηνύματα *SGSN Key Exchange* και *MS Key Exchange*.

viii. Το UE πρέπει να αποδείξει ότι κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιέχεται στο PKC, το οποίο έστειλε στο SGSN. Έτσι, το *Certificate Verify* μήνυμα περιέχει μια ψηφιακά υπογεγραμμένη σύνοψη των πληροφοριών (κλειδιά και μηνύματα), τα οποία είναι γνωστά και στα δύο μέρη. Η σύνοψη θα ελεγχθεί από το SGSN, κάνοντας χρήση του δημόσιου κλειδιού του UE.

ix. Το SGSN ελέγχει την εγκυρότητα του ψηφιακού πιστοποιητικού του UE διεξάγοντας αντίστοιχους έλεγχους με αυτούς του SGSN στο βήμα v.

x. Το SGSN αποκρυπτογραφεί την *pre-master* τιμή και το IMSI, χρησιμοποιώντας το ιδιωτικό του κλειδί. Κατόπιν, δημιουργεί μια τιμή P-TMSI.

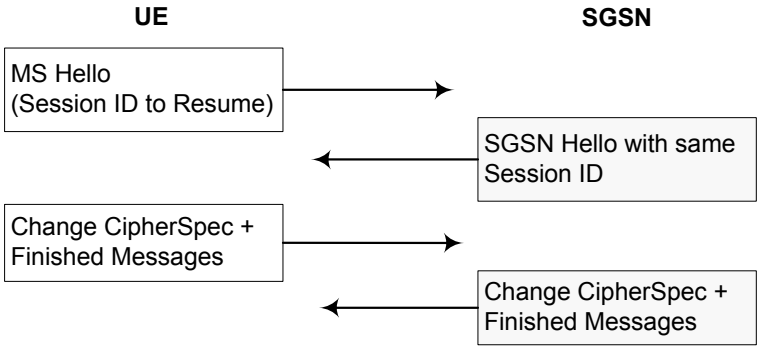
xi. Τα δύο μέρη μετατρέπουν την *pre-master* τιμή σε *master*. Οι διαδικασίες μετατροπής περιλαμβάνουν συνόψεις MD5 και SHA-1 με παραμέτρους εισόδου τις session ID τιμές. Το *master* κλειδί θα χρησιμοποιηθεί για κρυπτογράφηση και MAC υπολογισμούς.

xii. Το UE αποστέλλει στο SGSN τα μηνύματα Change CipherSpec και Finished και το SGSN απαντάει ανάλογα. Σημειώνεται, ότι τα *Finished* μηνύματα είναι προστατευμένα από εμπιστευτικότητα και ακεραιότητα με βάση τις συμφωνηθείσες παραμέτρους. Το *Attach accept* μήνυμα που στέλνεται από το SGSN στο UE περιλαμβάνει και το P-TMSI που δημιουργήθηκε στο βήμα x.

4.3.3. Διαδικασία ανανέωσης συνόδων AKA SSL

Με στόχο τη μείωση της επιβάρυνσης που προέρχεται από τις κρυπτογραφικές λειτουργίες και το σημαντικό πλήθος των μηνυμάτων που ανταλλάσσονται, το SSL ορίζει ένα μηχανισμό, με βάση τον οποίο οι επικοινωνούσες οντότητες μπορούν να χρησιμοποιήσουν παραμέτρους επικοινωνίας που συμφωνήθηκαν σε κάποια προηγούμενη σύνοδο. Όπως φαίνεται στο σχήμα 4-3, η διαδικασία ανανέωσης συνόδου μπορεί να επιταχύνει σημαντικά το πρωτόκολλο διαπραγμάτευσης του AKA SSL.

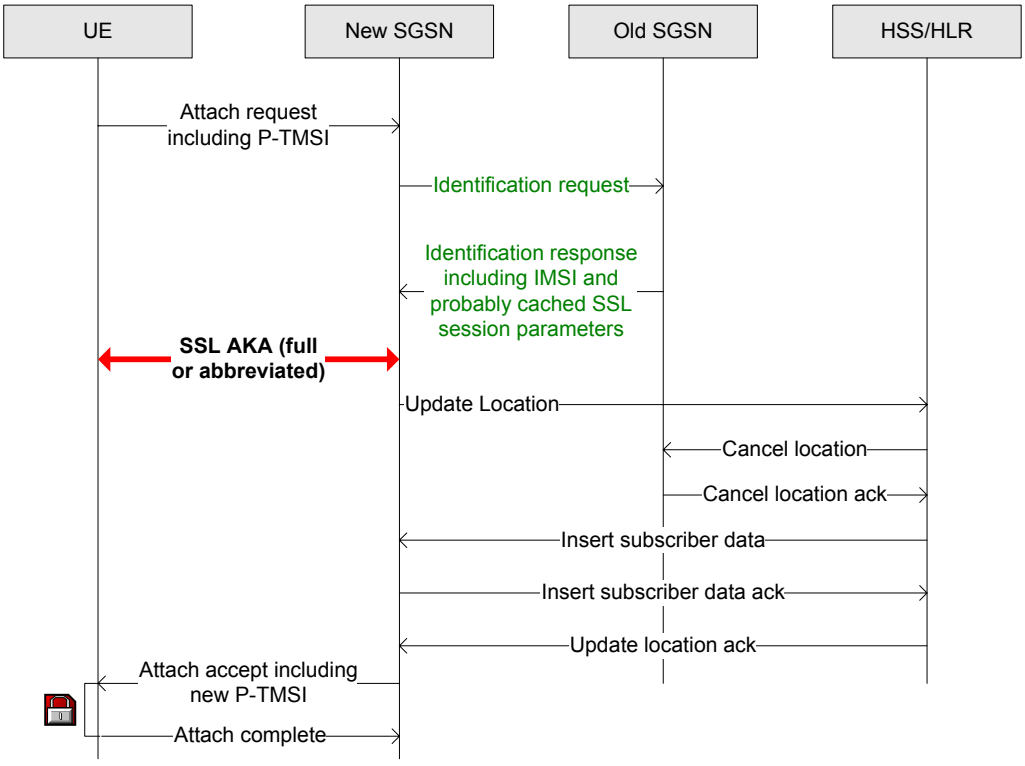
Τα δύο μηνύματα *Hello* προσδιορίζουν αν η σύνοδος μπορεί να ανανεωθεί ή όχι. Πιο συγκεκριμένα, αν το UE επιθυμεί να ανανεώσει μια από τις προηγούμενες συνόδους, τότε συμπεριλαμβάνει το αναγνωριστικό της συνόδου αυτής στο μήνυμα *UE Hello* προτείνοντάς την στο SGSN. Αν το SGSN συμφωνεί και διαθέτει τις παραμέτρους της εν λόγω συνόδου στην προσωρινή ή κρυφή (cache) του μνήμη, απαντάει με το ίδιο session ID στο δικό του μήνυμα *Hello*. Διαφορετικά δημιουργεί ένα νέο αναγνωριστικό συνόδου και τα δύο μέρη προχωρούν σε πλήρη διαπραγμάτευση (Rescorla, 2001; Thomas, 2000).



Σχήμα 4-3. Ανανέωση AKA SSL συνόδου (συντετμημένη χειραψία)

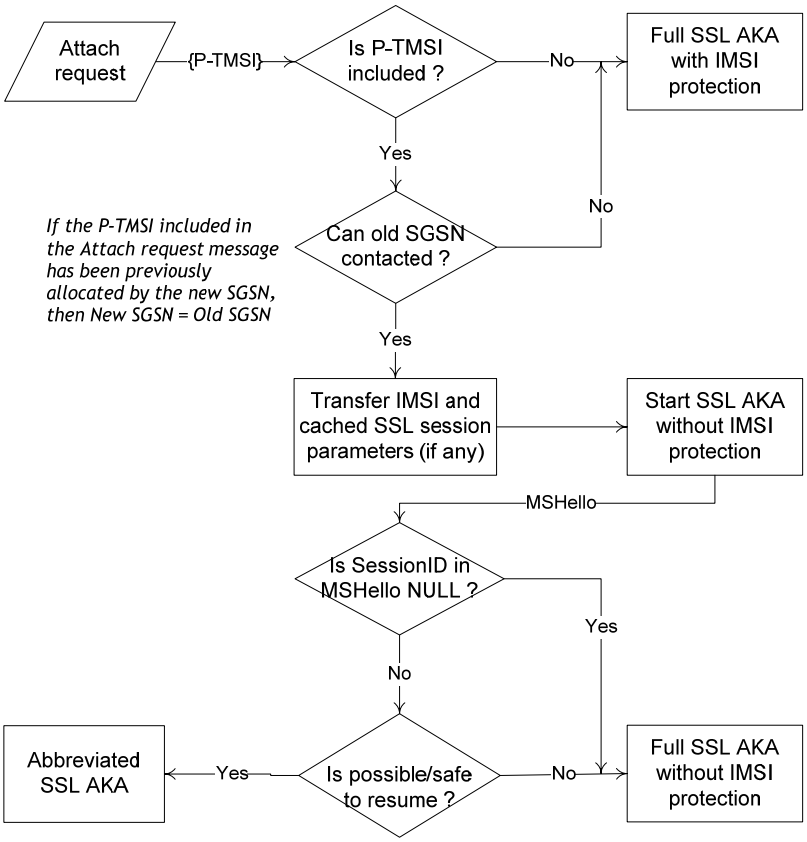
Ολόκληρη η διαδικασία σύνδεσης με το δίκτυο, η οποία ενσωματώνει τον προτεινόμενο μηχανισμό AKA SSL, παρουσιάζεται με τη μορφή διαγράμματος ακολουθίας μηνυμάτων στο σχήμα 4-4.

Το UE ανακαλεί το P-TMSI του, το οποίο είναι αποθηκευμένο στη μη-μεταβλητή (non-volatile) μνήμη του, το τοποθετεί στο μήνυμα αίτησης σύνδεσης με το δίκτυο και το αποστέλλει στο νέο SGSN. Το P-TMSI έχει εκχωρηθεί (allocated) στο UE, πιθανότατα από κάποιο άλλο SGSN (προηγούμενο SGSN) σε κάποια άλλη περιοχή δρομολόγησης (routing area). Εννοείται ότι αν το P-TMSI έχει εκχωρηθεί στο UE από το νέο SGSN, τότε νέο και προηγούμενο SGSN ταυτίζονται και το νέο SGSN ήδη γνωρίζει το IMSI του UE. Το κατά πόσο μια σύνοδος μπορεί να ανανεωθεί ή όχι παρουσιάζεται στο σχήμα 4-5, με τη μορφή ενός διαγράμματος ροής (decision flowchart).



Σχήμα 4-4. Διαδικασία σύνδεσης με το δίκτυο (attach procedure)

Αν και η διαδικασία ανανέωσης συνόδων βελτιώνει την αποτελεσματικότητα της AKA SSL διαδικασίας εξυπηρετώντας και τα δύο μέρη, οι πάροχοι θα πρέπει να είναι ιδιαίτερα προσεκτικοί στην εφαρμογή της. Όταν χρησιμοποιείται για μεγάλα χρονικά διαστήματα το ίδιο κλειδί για την κρυπτογράφηση των δεδομένων, το σύστημα αναπόφευκτα γίνεται όλο και λιγότερο ασφαλές. Οι πιθανοί εισβολείς αποκτούν όλο και περισσότερα δεδομένα και έχουν στη διάθεσή τους αρκετό χρόνο για να τα αναλύσουν. Έτσι, τα SGSNs πρέπει να θέσουν κάποιο άνω όριο (threshold) στον επιτρεπτό αριθμό επαναλήψεων μιας συνόδου, όπως και στο χρονικό διάστημα που μεσολαβεί μεταξύ διαδοχικών επαναλήψεων της ίδιας συνόδου. Αν κάποιος από τους παραπάνω περιορισμούς δεν ικανοποιείται, τότε τα συστήματα πρέπει να υποχρεώνονται σε πλήρη διαπραγμάτευση (full negotiation).



Σχήμα 4-5. Διαδικασία ελέγχου για τον αν μια AKA SSL σύνοδος μπορεί να ανανεωθεί

4.3.4. AKA SSL σε συνεργαζόμενο δίκτυο (SN)

Στην περίπτωση που κάποιος συνδρομητής περιάγει σε συνεργαζόμενο με το HN δίκτυο, η διαδικασία SSL AKA παραμένει ως έχει, με την προϋπόθεση ότι οι CAs των δύο δικτύων έχουν αλληλο-πιστοποιηθεί. Τότε το SGSN είναι υποχρεωμένο να αποστείλει το αντίστοιχο cross-reference πιστοποιητικό στο UE. Μια άλλη λύση είναι η ύπαρξη κοινής έμπιστης CA για τα δύο (ή για *n* στη γενική περίπτωση) δίκτυα, η οποία λειτουργεί ως CSP. Μια ιεραρχική

οργάνωση των CA, ικανή να υποστηρίξει και τις δια-δικτυακές σχέσεις εμπιστοσύνης μεταξύ των παρόχων, μπορεί επίσης να αποτελέσει μια αξιόπιστη επιλογή.

4.3.5. Πρόσθετες Απαιτήσεις

Εκτός αυτών που συζητήθηκαν παραπάνω, η εισαγωγή του μηχανισμού AKA SSL απαιτεί τη διερεύνηση κάποιων πρόσθετων ζητημάτων. Με βάση τις ισχύουσες 2.5G προδιαγραφές, ο προτεινόμενος μηχανισμός δεν είναι δυνατό να υλοποιηθεί, διότι δεν υπάρχει (ευθεία) IP συνδεσιμότητα (connectivity) μεταξύ UE και SGSN. Παρόλα αυτά, ένα 3G-SGSN θα επικοινωνεί προς όλες τις κατευθύνσεις (RNC, GGSN), χρησιμοποιώντας το πρωτόκολλο IP και γι' αυτό το λόγο είναι πολύ πιθανό ότι τελικά θα ενοποιηθεί λειτουργικά με το GGSN. Ανεξάρτητα επίσης από το ποια οντότητα δικτύου θα παρέχει υπηρεσίες AKA, πιστεύουμε ότι είναι περισσότερο αποδοτικό η AKA διαδικασία να υλοποιηθεί ως υπηρεσία, η οποία θα προσφέρεται στο χρήστη ανεξάρτητα από το δίκτυο (access network/domain) που αυτός συνδέεται και την υπηρεσία που επιθυμεί να αποκτήσει.

Για παράδειγμα, όπως είδαμε στην ενότητα 3.3.3, ο μηχανισμός 3GPP AKA χρησιμοποιείται για την αυθεντικοποίηση των χρηστών στο ασύρματο δίκτυο (radio network) αλλά και το πολυμεσικό υποσύστημα του UMTS. Επιπλέον, οι 3GPP προδιαγραφές για την έκδοση 6 του UMTS, περιγράφουν μια δια-δικτυακή αρχιτεκτονική μεταξύ UMTS και WLAN, στην οποία το HN διενεργεί έλεγχο προσπέλασης (access control), ενώ ένας 3GPP proxy μεταβιβάζει τη σχετική σηματοδοσία σε ένα AAA εξυπηρέτη στο HN. Η 3GPP φαίνεται να επιλέγει το πρωτόκολλο Extensible Authentication Protocol (EAP)-AKA για να υποστηρίξει τη διασύνδεση με WLAN δίκτυα (3GPP TS, 2003b, 3GPP TS, 2002d, Arkko & Haverinen, 2003).

Σε αυτό το B3G περιβάλλον αντιλαμβανόμαστε την αυθεντικοποίηση ως υπηρεσία η οποία διενεργείται κάτω από το επίπεδο εφαρμογής, ανεξάρτητα από την υπάρχουσα τεχνολογία δικτύου. Αλλά και σύμφωνα με την *all-IP* προοπτική, μια «ανεξαρτήτως τεχνολογίας» προσέγγιση θα ήταν ενδεχομένως η καταλληλότερη.

Εξίσου σημαντικό ζήτημα αποτελεί το γεγονός ότι η διαδικασία AKA SSL προστατεύει με επιτυχία τα δεδομένα του χρήστη, αλλά αφήνει απροστάτευτη τη σηματοδοσία μεταξύ UE και RNC. Παρόλα αυτά, τα κλειδιά κρυπτογράφησης και ακεραιότητας που δημιουργήθηκαν κατά την AKA SSL χειραψία μπορούν να χρησιμοποιηθούν για την προστασία της σηματοδοσίας στα χαμηλότερα επίπεδα. Η διαδικασία είναι παρόμοια με αυτή που ορίζεται στις τρέχουσες UMTS προδιαγραφές, για την προστασία της εμπιστευτικότητας και της ακεραιότητας στα δεδομένα σηματοδοσίας. Ένας ανάλογος μηχανισμός με το μήνυμα "*The security mode command*" του πρωτοκόλλου Radio Access Network Application Protocol (RANAP) (3GPP TS, 2002c) είναι απαραίτητος για να μεταφέρει τα απαραίτητα κλειδιά στο RNC μετά το τέλος της χειραψίας. Επίσης, η κρυπτογράφηση των δεδομένων σηματοδοσίας μπορεί να

θεωρηθεί προαιρετική, μιας και το σημαντικό ζήτημα γι' αυτά είναι η προστασία της ακεραιότητάς τους. Επιπλέον, η USIM εφαρμογή θα πρέπει να υποστηρίζει τους αλγορίθμους *f8* και *f9* για την κρυπτογράφηση και την προστασία της ακεραιότητας των δεδομένων της σηματοδοσίας αντίστοιχα.

4.4. Πειραματική ανάλυση και αξιολόγηση του μηχανισμού AKA SSL

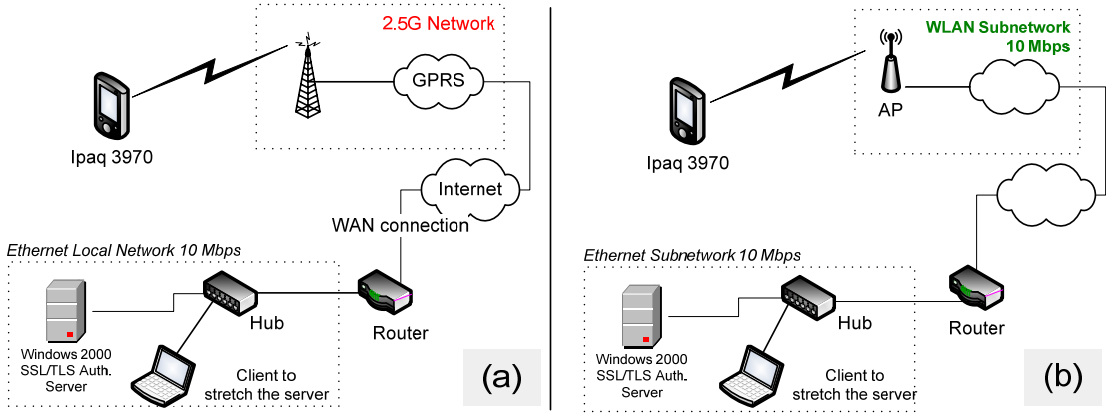
4.4.1. Περιγραφή του πειράματος

Προκειμένου να αξιολογήσουμε το μηχανισμό AKA SSL, κατασκευάσαμε μια πρότυπη αρχιτεκτονική υλικού και λογισμικού. Ο κύριος στόχος ήταν να δείξουμε ότι ο συγκεκριμένος μηχανισμός είναι υλοποιήσιμος από την άποψη του χρόνου εξυπηρέτησης, με βάση τα σημερινά αλλά και τα μελλοντικά τεχνολογικά δεδομένα. Η τοπολογία του περιγράφεται στο σχήμα 4-6(a). Η κινητή συσκευή που χρησιμοποιήσαμε ήταν ένας υπολογιστής τσέπης (Pocket PC, PPC), της εταιρείας Compaq με τύπο iPAQ H3970. Το συγκεκριμένο PPC είχε εγκατεστημένο το λειτουργικό σύστημα Windows PPC 2002 της Microsoft.

Στην πρόσθετη υποδοχή PCMCIA (expansion pack) του PPC είχε τοποθετηθεί η κάρτα D211 της εταιρείας Nokia, η οποία μπορεί να συνδέεται τόσο σε δίκτυα GPRS class 7, όσο και σε δίκτυα τεχνολογίας WLAN IEEE 802.11b. Το PPC ενσωματώνει επεξεργαστή της εταιρείας Intel του τύπου X-Scale PXA250 με ταχύτητα 400 MHz, ενώ διαθέτει 64 MB κύριας (RAM) και 48 MB βοηθητικής μνήμης (flash ROM) αντίστοιχα. Τα 22 MB από τα 48 MB συνολικά της βοηθητικής μνήμης παραμένουν στη διάθεση του χρήστη για την αποθήκευση εφαρμογών και άλλων αρχείων. Από την άλλη πλευρά, ο εξυπηρέτης ενσωματώνει δύο παράλληλους επεξεργαστές Pentium III με ταχύτητα 600 MHz, ενώ διαθέτει 256 MB κύριας μνήμης την οποία διαχειρίζεται το λειτουργικό σύστημα Windows 2000 SP4 της εταιρείας Microsoft. Ο εξυπηρέτης διαθέτει επίσης μόνιμη σύνδεση με το Διαδίκτυο (WAN connection). Ανάλογες και συγκρίσιμες με την προηγούμενη τοπολογίες μπορούν να βρεθούν στη βιβλιογραφία (Chakravorty & Pratt, 2002; Chakravorty et al., 2002; Korhonen et al., 2001).

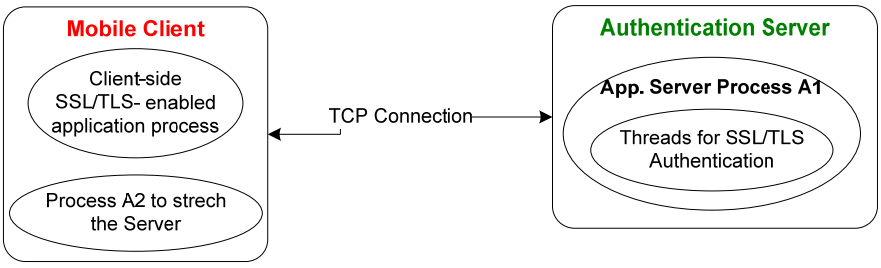
Οι εφαρμογές που χρησιμοποιήθηκαν αναπτύχθηκαν με τη γλώσσα Embedded C++ της Microsoft στην έκδοση 4.0. Προκειμένου επίσης να ενσωματώσουμε την απαραίτητη SSL λειτουργικότητα στις εφαρμογές μας, χρησιμοποιήσαμε το πακέτο ανοικτού κώδικα (open-source) OpenSSL (www.openssl.org) στην έκδοση 0.9.7b (Viega et al., 2002; Rescorla, 2001). «Ελαφρύτερα» (lightweight) SSL πακέτα λογισμικού, όπως η Java 2 Micro Edition (J2ME), ή Kilobyte-SSL της εταιρείας Sun και η Bsafe SSL-C/SSL-J της εταιρείας RSA, προσφέρουν μεν αυθεντικοποίηση με χρήση ψηφιακών πιστοποιητικών αλλά μόνο από την πλευρά του εξυπηρέτη. Επιπλέον, η απόδοση (σε ταχύτητα εκτέλεσης κρυπτογραφικού κώδι-

κα) της γλώσσας προγραμματισμού Java, είναι κατά πολύ υποδεέστερη απ' αυτή της γλώσσας C++.



Σχήμα 4-6. Η τοπολογία που αξιοποιήθηκε

Η αρχιτεκτονική του λογισμικού παρουσιάζεται στο σχήμα 4-7. Στον SSL εξυπηρέτη αυθεντικοποίησης εκτελείται η διεργασία (process) A1, η οποία ενεργοποιεί ένα TCP-SSL listening socket και αναμένει για συναλλαγές (transactions). Η A1 είναι πολυ-νηματική (multi-threaded). Όταν λαμβάνει ένα μήνυμα για SSL συναλλαγή ενεργοποιεί ένα νήμα για να ανταποκριθεί και να το εξυπηρετήσει. Η διεργασία A2 εκτελείται σε μια διαφορετική μηχανή με σκοπό να παράγει ένα μεγάλο αριθμό SSL αιτήσεων και έτσι να δημιουργήσει εικονικό φόρτο επεξεργασίας στον SSL εξυπηρέτη. Ο χρόνος μεταξύ δύο διαδοχικών SSL αιτήσεων για εξυπηρέτηση ακολουθεί την αρνητικά εκθετική κατανομή (negative exponential distribution).

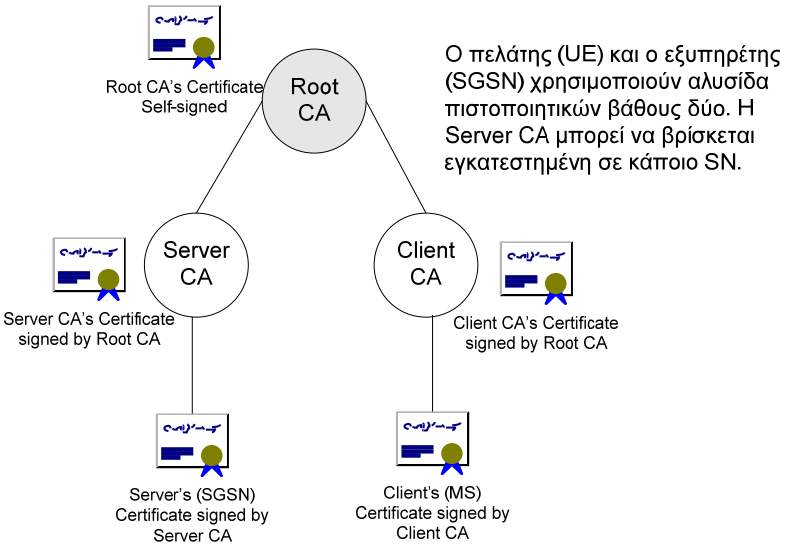


Σχήμα 4-7. Η πειραματική αρχιτεκτονική του λογισμικού

Προσπαθήσαμε να ελαχιστοποιήσουμε τις απαιτήσεις της εφαρμογής-πελάτη σε υπολογιστικούς πόρους και μνήμη, αφαιρώντας από τις εφαρμογές μας κλήσεις (calls) σε δευτερεύουσας σημασίας, απαιτητικές όμως σε πόρους, OpenSSL συναρτήσεις. Γι' αυτό το λόγο, αφήσαμε εκτός κλήσεις σε συναρτήσεις οι οποίες φορτώνουν βιβλιοθήκες με μηνύματα λαθών, επαληθεύουν μονοπάτια (paths), στα οποία βρίσκονται αποθηκευμένα τα ψηφιακά πιστοποιητικά του πελάτη και αλυσίδες πιστοποιητικών μήκους μεγαλυτέρου των τεσσάρων. Επίσης, τροποποιήσαμε τις εφαρμογές ώστε να παρέχουν υποστήριξη μόνο για SSL συνδέσεις έκδοσης 3.0 (version 3.0) και TLS έκδοσης 1.0. Επίσης, αφαιρέσαμε την υποστήριξη για αλγορίθμους

κρυπτογράφησης και υπολογισμού MAC, οι οποίοι επιτρέπουν ανώνυμες συνδέσεις (anonymous) ή είναι αδύνατοι (weak), όπως ο αλγόριθμος MD5.

Η διαδικασία χειραψίας και αυθεντικοποίησης είναι αμοιβαία. Ο πελάτης (UE) και ο εξυπηρέτης (SGSN) ανταλλάσσουν τα πιστοποιητικά τους, τα οποία είναι τοπικά αποθηκευμένα μαζί με τα δημόσια κλειδιά των έμπιστων CAs. Αποφασίσαμε να αξιολογήσουμε ένα σενάριο αυθεντικοποίησης σε SN, «πιέζοντας» (stretching) έτσι τον πελάτη ακόμη περισσότερο. Γι' αυτό, χρησιμοποιήσαμε μια αλυσίδα πιστοποιητικών βάθους 2, όπως αυτή παρουσιάζεται στο σχήμα 4-8. Και τα δύο μέρη ελέγχουν τα πιστοποιητικά ως προς το χρόνο λήξης τους και την αρχή πιστοποίησης που τα έχει εκδώσει. Αντίθετα, δε διενεργείται κάποιος έλεγχος για το αν τα πιστοποιητικά έχουν συμπεριληφθεί σε κάποια σχετική λίστα ανάκλησης (CRL). Στην πραγματικότητα υποχρεωμένος για κάτι τέτοιο είναι μόνον ο εξυπηρέτης, ελέγχοντας το P-TMSI που αποστέλλει το UE. Αυτό προϋποθέτει κάποια διαδικασία σύγκρισης του P-TMSI με το αντίστοιχο IMSI.



Σχήμα 4-8. Αλυσίδα πιστοποιητικών βάθους 2

Όλα τα κλειδιά RSA που χρησιμοποιήθηκαν είχαν μήκος 1024 bits, ενώ η ανταλλαγή του *pre-master* μυστικού βασίστηκε στον αλγόριθμο *ephemeral Diffie-Hellman* (Rescorla, 1999) με RSA υπογραφές. Η χρήση του παραπάνω αλγορίθμου εξασφαλίζει «μελλοντική μυστικότητα» (forward secrecy). Τα δύο μέρη δημιουργούν συμμετρικό κλειδί SSL ή TLS συνόδου μήκους 128 ή 256 bits (για AES256) αντίστοιχα. Οι πλήρεις σουίτες αλγορίθμων που χρησιμοποιήσαμε στις εφαρμογές μας ήταν: EDH-RSA για ανταλλαγή *pre-master* κλειδιών μήκους 512 ή 1024 bits, DES-CBC3 ή AES256 για κρυπτογράφηση και SHA για συνόψεις. Οι παραπάνω σουίτες θεωρούνται σημαντικά «βαρύτερες» (heavy), συγκρινόμενες για παράδειγμα, με τις γρηγορότερες αλλά πιο «αδύνατες» (RSA_RC4_128_MD5 και RSA_RC4_40_MD5) της Kilobyte-SSL.

Το σχήμα 4-6(b) παρουσιάζει την αρχιτεκτονική υλικού που χρησιμοποιήσαμε προκειμένου να εκτιμήσουμε την απόδοση του ίδιου μηχανισμού σε δίκτυο του τύπου 802.11b. Οι συνθήκες διεξαγωγής των πειραμάτων σ' αυτή την περίπτωση, συμπεριλαμβανομένων των μηχανών πελάτη και εξυπηρέτη και των αντίστοιχων εφαρμογών και ρυθμίσεων, παραμένουν ίδιες. Επιπλέον, χρησιμοποιήσαμε ένα σημείο πρόσβασης (Access Point, AP) της εταιρείας D-Link με τύπο DWL-900AP+, προκειμένου να επιτύχουμε σύνδεση με το 802.11b (WLAN) υπο-δίκτυο.

4.4.2. Αποτελέσματα Μετρήσεων

Εκτελέσαμε τους υπολογισμούς κατά τη διάρκεια διαφορετικών ημερών σε ώρες αιχμής (peak hours), χρησιμοποιώντας διάφορες τιμές για το ρυθμό αφίξεων λ της διεργασίας A2, η οποία «φορτώνει» τη διεργασία (A1) του εξυπηρέτη με AKA SSL αιτήσεις. Το GPRS σχήμα κωδικοποίησης (coding scheme) ήταν CS-1 (9.05 kb/s) και οι διαθέσιμες για το GPRS «θυρίδες χρόνου» (time slots) μεταβάλλονταν μεταξύ 3 και 4. Ως αποτέλεσμα, η ταχύτητα του ασύρματου δικτύου κυμαινόταν από 27 έως 36 Kb/s. Καταγράψαμε μετρήσεις για τους ακόλουθους χρόνους που αφορούν τη διεργασία του πελάτη.

i. Χρόνος απόκρισης δικτύου (*NRT*): Ο χρόνος που απαιτείται για να ολοκληρωθεί η σύνδεση με την υποδοχή (socket) του εξυπηρέτη. Αυτός ο χρόνος περιλαμβάνει ένα round-trip δικτύου και τους σχετικούς με την αποδοχή της κλήσης χρόνους επεξεργασίας στον πελάτη και στον εξυπηρέτη.

ii. Χρόνος προετοιμασίας της αίτησης (*RPT*): Ο συνολικός χρόνος που παρήλθε πριν ξεκινήσει η διαδικασία χειραψίας. Αυτός ο χρόνος περιλαμβάνει το χρόνο NRT και το χρόνο προετοιμασίας. Για παράδειγμα, τον απαραίτητο χρόνο για το UE να φορτώσει τα πιστοποιητικά στη μνήμη.

iii. Συνολικός χρόνος χειραψίας (*THT*): Ο χρόνος που μεσολαβεί από το μήνυμα *UE Hello*, μέχρι το μήνυμα *finished*.

iv. Συνολικός χρόνος κλήσης (*TST*): Ο χρόνος που παρήλθε από την αρχή της επικοινωνίας, μέχρι τα δύο μέρη να έχουν δημιουργήσει το συμμετρικό κλειδί και έτσι να είναι έτοιμα να ξεκινήσουν την ανταλλαγή δεδομένων. Ο χρόνος αυτός είναι το άθροισμα των RPT και THT.

Στην πλευρά του εξυπηρέτη καταγράψαμε τον ακόλουθο χρόνο:

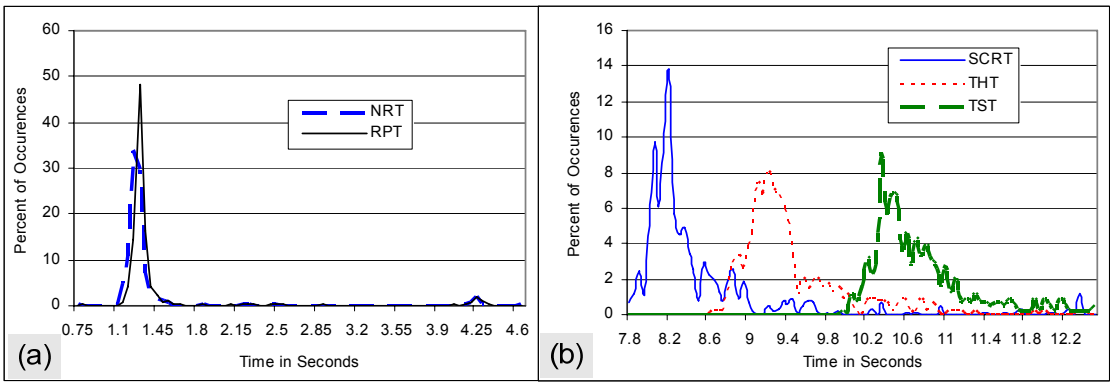
v. Χρόνος εξυπηρέτησης αίτησης (*SCRT*): Ο χρόνος που μεσολαβεί από το μήνυμα *Hello* του εξυπηρέτη μέχρι η αίτηση να έχει εξυπηρετηθεί.

Κατά τη διάρκεια των πειραμάτων, καταγράψαμε 1000 μετρήσεις των προαναφερόμενων χρόνων, από ένα ίσο πλήθος συναλλαγών που εκκινήθηκαν από τον πελάτη μας. Οι μέσοι όροι και οι διακυμάνσεις των μετρήσεων για καθένα από τους παραπάνω χρόνους (i έως v), παρουσιάζονται στον πίνακα 4-1 σε msec. Επίσης, τα διαγράμματα των συναρτήσεων πυκνότητας πιθανοτήτων (probability density function, PDF) αυτών των τιμών παρουσιάζονται στα σχήματα 4-9(a) και 4-9(b).

	UE (iPAQ) (ms)				*Εξυπηρέτης (ms)*
	NRT	RPT	THT	TST	SCRT
M.O. (Average)	1391	1427	9480	10950	8469
Διακύμανση (S.D.)	610	620	750	980	760

Πίνακας 4-1. Χρόνοι εξυπηρέτησης σε GPRS (iPAQ\GPRS)

Στο σχήμα 4-9(a), μπορούμε να διακρίνουμε τη σχέση μεταξύ των χρόνων NRT και RPT. Παρατηρούμε ότι η καμπύλη του RPT αποτελεί στην ουσία μετατόπιση της καμπύλης του NRT κατά περίπου 0.1 δευτερόλεπτο. Αυτό σημαίνει ότι η διαδικασία προετοιμασίας είναι σταθερή (και αμελητέα) και ο χρόνος πριν την εκκίνηση της χειραψίας εξαρτάται εξ ολοκλήρου από την κατανομή του NRT π.χ. την ταχύτητα του δικτύου.



Σχήμα 4-9. PDF διαγράμματα χρόνων εξυπηρέτησης στο GPRS (iPAQ\GPRS)

Ομοίως, στο σχήμα 4-9(b), παρουσιάζουμε τη σχέση μεταξύ των χρόνων TST, THT και SCRT. Παρατηρούμε ότι η THT καμπύλη είναι μετατοπισμένη δεξιά του SCRT κατά 1 περίπου δευτερόλεπτο. Ο χρόνος αυτός, περιλαμβάνει μισό round-trip χρόνο δικτύου (0.7 sec) από το αρχικό μήνυμα UE Hello. Και οι τρεις καμπύλες έχουν περίπου την ίδια κατανομή. Αυτό δικαιολογείται από το γεγονός ότι το πρωτόκολλο απαιτεί 10 συνολικά ανταλλαγές ή περίπου 5 NRT χρόνους. Κατά συνέπεια, πολλαπλασιάζοντας το μέσο χρόνο των 1301 ms που απαιτείται για ένα round-trip δικτύου επί 5, έχουμε συνολικά 7 δευτερόλεπτα. Αν σ' αυτά προσθέσουμε τους διάφορους άλλους χρόνους που απαιτούνται για υπολογισμούς, επαληθεύσεις και συνόψεις, καταλήγουμε στα 10.95 δευτερόλεπτα του μέσου TST. Σημειώνεται επί-

σης, ότι οι μετρήσεις δεν έδειξαν να επηρεάζονται από το φόρτο που δημιουργούσε στον εξυπηρέτη η διεργασία A2.

Επιπλέον, ο πίνακας 4-2, παρουσιάζει τις απαιτήσεις του UE σε πόρους μνήμης (Kilobytes), όπως αυτές καταγράφηκαν στα πειράματά μας. Οι τιμές αυτές είναι ενδεικτικές για μια φορητή συσκευή προκειμένου αυτή να είναι ικανή να εκτελέσει το μηχανισμό AKA SSL.

Χαρακτηριστικό	*Μνήμη που απαιτείται (KB)*
Δίσκος ή Flash ROM για τα αρχεία OpenSSL.dll	1132
Δίσκος ή Flash ROM για την εφαρμογή του UE	16
EPROM μνήμη στη UICC για την αποθήκευση των πιστοποιητικών (ομοίως για τον εξυπηρέτη)	4.07
EPROM μνήμη στη UICC για ένα πιστοποιητικό (ρίζας) έμπιστης CA	1.02
RAM μνήμη για τη διεργασία στον εξυπηρέτη	100

Πίνακας 4-2. Απαιτήσεις σε μνήμη για το UE και τον εξυπηρέτη

4.4.3. Σχόλια επί των αποτελεσμάτων

Ο μέσος όρος των σχεδόν 11 δευτερολέπτων, όπως αυτός εμφανίζεται στον Πίνακα 1-4, οπωσδήποτε και δεν μπορεί να είναι αποδεκτός από ένα χρήστη 3G ή B3G υπηρεσιών. Παρόλα αυτά, συγκρίνοντας τη τιμή του TST με την αντίστοιχη μιας WTLS υπηρεσίας, παρατηρούμε ότι σε αρκετές περιπτώσεις το WTLS είναι ακόμα πιο αργό. Επίσης, συγκρίσιμα αποτελέσματα με Kilobyte-SSL, 20 MHz Palm επεξεργαστή και χρήση πιστοποιητικών μόνο από την πλευρά του πελάτη, δείχνουν χρόνους γύρω στα 10 δευτερόλεπτα (Gupta, 2002).

Εκτός της προαναφερόμενης, δύο ακόμη εργασίες περιγράφουν και αξιολογούν παρόμοιους μηχανισμούς αυθεντικοποίησης βασισμένους σε δημόσιο κλειδί για 3G ή B3G συσκευές. Η πρώτη (Al-Muhtadi et al., 2002), προτείνει μια εναλλακτική υλοποίηση της αρχιτεκτονικής SESAME, η οποία είναι γνωστή ως Tiny SESAME. Το SESAME αποτελεί επέκταση του πρωτοκόλλου Kerberos, παρέχοντας πρόσθετες υπηρεσίες. Οι μετρήσεις βασίστηκαν σε PPC τύπου Jornada 680 της εταιρείας HP, το οποίο ενσωματώνει επεξεργαστή ταχύτητας 133 MHz και λειτουργικό σύστημα CE 2.11 της εταιρείας Microsoft. Η έκδοση του Tiny SESAME που εγκαταστάθηκε στη φορητή συσκευή για τις ανάγκες των πειραμάτων, είχε υλοποιηθεί στη γλώσσα PersonalJava.Τα αποτελέσματα έδειξαν χρόνους αυθεντικοποίησης από 10 έως 16 δευτερόλεπτα ανάλογα με το (κατά περίπτωση) σχήμα κλήσης (call setup scheme). Η δεύτερη (Harbitter & Menasce, 2001) χρησιμοποιεί αρχιτεκτονική Kerberos υπο-

βοηθούμενη από proxy διαμεσολαβητές μεταξύ του πελάτη και του εξυπηρέτη. Οι μετρήσεις έγιναν σε PPC τύπου Vadem Clio C-1000, το οποίο ενσωματώνει επεξεργαστή ταχύτητας 100 MHz και λειτουργικό σύστημα Windows CE. Οι εφαρμογές είχαν υλοποιηθεί σε γλώσσα C++. Τα αποτελέσματα έδειξαν χρόνους αυθεντικοποίησης μεταξύ 8 και 15 δευτερολέπτων ανάλογα με το σενάριο και την ταχύτητα του δικτύου.

Εκτός από τις παραπάνω παρατηρήσεις μπορούμε να αναφέρουμε τα εξής:

- Πρέπει να λάβουμε υπόψη ότι η ταχύτητα των 3G δικτύων θα κυμαίνεται από 144 Kbps έως 384 Kbps για ευρεία (wide) και 2 Mbps για χαμηλή (low) κάλυψη (coverage) και κινητικότητα (mobility). Ως αποτέλεσμα αναμένεται σημαντική μείωση των σχετικών round-trip χρόνων. Για παράδειγμα, υποθέτοντας ταχύτητα δικτύου 144 Kbps και εκτελώντας πρόχειρους υπολογισμούς, ο χρόνος NRT μειώνεται σε 200.8 ms, δείχνοντας μια βελτίωση 400%.

- Ένα καλύτερο GPRS σχήμα κωδικοποίησης (coding scheme), εφόσον αυτό ήταν διαθέσιμο από τον πάροχο και ήταν επιτρεπτό στις υφιστάμενες συνθήκες σύνδεσης, θα ήταν δυνατό να βελτιώσει σε σημαντικό βαθμό τη διαδικασία χειραψίας (Korhonen et al., 2001).

- Πρέπει επίσης να υπολογίσουμε την πρόσθετη καθυστέρηση δικτύου που προήλθε από το γεγονός ότι ο εξυπηρέτης μας δεν ήταν εγκατεστημένος στο κεντρικό δίκτυο του παρόχου υπηρεσιών 2.5G. Χρησιμοποιώντας εργαλείο ping ανακαλύψαμε ότι η πρόσθετη αυτή επιβάρυνση για κάθε round-trip ήταν περίπου 200 ms.

- Επίσης πρέπει να λάβουμε υπόψη μας ότι τα ψηφιακά πιστοποιητικά που ανταλλάσσονται από τα δύο μέρη, σύμφωνα με το σενάριο μας, προσφέρονται για αυθεντικοποίηση σε SN. Με βάση τις τρέχουσες προδιαγραφές των 2.5G και 3G δικτύων, το SN θα πρέπει να ζητήσει διανύσματα αυθεντικοποίησης από το HN ενός συνδρομητή προκειμένου να είναι σε θέση να τον αυθεντικοποιήσει. Σημειώνεται επίσης ότι μια συνήθης 2.5G διαδικασία αυθεντικοποίησης σε SN διαρκεί κατά μέσο όρο από 5 έως 7 δευτερόλεπτα.

Τυχόν βελτιώσεις στο μηχανισμό AKA SSL μπορεί να προέλθουν είτε από την πρόοδο στην τεχνολογία σχεδιασμού και κατασκευής φορητών συσκευών είτε από βελτιστοποιήσεις στη δομή του πρωτοκόλλου ή στην αρχιτεκτονική του δικτύου. Όπως είδαμε στην ενότητα 4.3.3, η δυνατότητα ανανέωσης συνόδων SSL μπορεί να βελτιώσει σημαντικά τους χρόνους εξυπηρέτησης. Η βελτίωση αυτή προέρχεται κυρίως από το γεγονός ότι οι επαναλαμβανόμενες σύνοδοι χρησιμοποιούν το ίδιο *master secret*, μειώνοντας κατ' αυτόν τον τρόπο τον υπολογιστικό φόρτο και τον αριθμό των μηνυμάτων που τα δύο μέρη ανταλλάσσουν. Γι' αυτό το λόγο, προσαρμόσαμε κατάλληλα τις εφαρμογές του πελάτη και του εξυπηρέτη έτσι ώστε να υποστηρίζουν ανανέωση συνόδων. Επαναλάβαμε τους υπολογισμούς και οι σχετικές μετρήσεις έδειξαν μέσον όρο για το χρόνο THT, 2.1 δευτερόλεπτα, δηλαδή βελτίωση 77%. Σχετικές

μελέτες με χρήση 512 bytes RSA κλειδιών παρουσιάζουν βελτίωση στην απόδοση της τάξης του 20X, ενώ ακόμη καλύτερη απόδοση επιτυγχάνεται, όταν χρησιμοποιούνται μεγαλύτερα σε μήκος κλειδιά (Rescorla, 2001).

Επιπλέον, η ανανέωση όλο και περισσότερων συνόδων αναμένεται να επιφέρει σημαντική βελτίωση και στη συνολική απόδοση (throughput) του δικτύου. Πρόσφατες εργασίες έδειξαν ότι ο μηχανισμός ανανέωσης συνόδων είναι εφικτό να βελτιωθεί ακόμα περισσότερο, χρησιμοποιώντας ένα SSL διεκπεραιωτή συνόδων (session aware dispatcher), όταν ο πάροχος σχεδιάζει την εγκατάσταση μιας συστοιχίας (cluster) εξυπηρετών αυθεντικοποίησης (Apostolopoulos et al., 2000). Επίσης, όπως αναφέρθηκε στην ενότητα 4.2, το πρωτόκολλο χειραψίας του SSL είναι δυνατό να βελτιωθεί έως και 7 φορές (Potlapally et al., 2002).

Κατά τη διάρκεια της SSL χειραψίας, ο εξυπηρέτης είναι πολλές φορές υποχρεωμένος να περιμένει για ένα μήνυμα από τον πελάτη και αντίστροφα. Το OpenSSL, για παράδειγμα, μπορεί να ενταμιεύσει (buffer) την έξοδο προς το δίκτυο προκειμένου να επιτύχει καλύτερες αποδόσεις. Έτσι, ορισμένες φορές είναι υπολογιστικά φθηνότερο και δικτυακά γρηγορότερο (λαμβάνοντας υπόψη τους round-trip χρόνους), να δημιουργούμε έναν αριθμό μηνυμάτων και κατόπιν να τα μεταδίδουμε όλα μαζί την ίδια στιγμή (Rescorla, 2001). Η απλούστερη τεχνική ενταμίευσης, που θα μπορούσε να εφαρμοστεί, είναι η χρήση ενός σταθερού στο μέγεθος ενταμιευτή. Όταν αυτός γεμίζει, τα περιεχόμενά του θα μεταδίδονται άμεσα στο δίκτυο. Είναι επίσης απαραίτητο να αδειάζουμε (flush) τον ενταμιευτή μετά από κάθε μετάδοση. Ο κρισιμότερος πάντως παράγοντας είναι η επιλογή του μεγέθους του ενταμιευτή, μιας και σε ορισμένες περιπτώσεις βελτιώνει την αναμονή (latency), ενώ σε κάποιες άλλες την χειροτερεύει.

4.4.4. Βελτιώνοντας την απόδοση του πελάτη

Θεωρήσαμε σημαντικό να μετρήσουμε πόσο η επεξεργαστική ισχύς του πελάτη (UE) μπορεί να επηρεάζει τη συνολική απόδοση του μηχανισμού AKA SSL. Γι' αυτό το λόγο, αντικαταστήσαμε το iPAQ με ένα φορητό υπολογιστή της εταιρείας Compaq, ο οποίος ενσωματώνει επεξεργαστή Pentium 4 χρονισμένο στα 2.2 GHz και 256 MB κύριας μνήμης. Η αρχική τοπολογία του δικτύου, (βλ. ενότητα 4.4.1) καθώς και οι υπόλοιπες ρυθμίσεις, παρέμειναν ίδιες. Καταγράψαμε έτσι ένα νέο σύνολο 1000 μετρήσεων από τους προαναφερόμενους χρόνους για ένα ίσο πλήθος συναλλαγών που εκκινήθηκαν από το φορητό υπολογιστή.

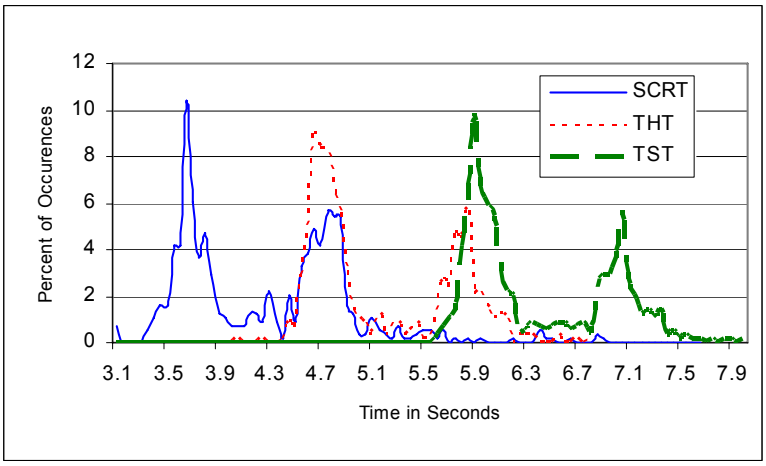
Τα αποτελέσματα των μετρήσεων παρουσιάζονται στον πίνακα 4-3, ενώ τα αντίστοιχα PDF διαγράμματα στο σχήμα 4-10.

Παρατηρούμε ότι ο μέσος RPT χρόνος ισούται με τον αντίστοιχο του NRT. Αυτό σημαίνει ότι ο χρόνος προετοιμασίας είναι στην ουσία μηδενικός, κάτι που άλλωστε είναι αναμενόμε-

νο για την πολύ γρήγορη μηχανή των 2.2 GHz. Για μια ακόμα φορά και οι τρεις καμπύλες παρουσιάζουν την ίδια κατανομή.

	UE (Φορητός Υπολογιστής) (ms)				*Εξυπηρέτης (ms)*
	NRT	RPT	THT	TST	SCRT
M.O. (Average)	1342	1343	5503	6840	4354
Διακύμανση (S.D.)	574	574	1298	1381	793

Πίνακας 4-3. Χρόνοι εξυπηρέτησης σε GPRS (Φορητός Υπολογιστής\GPRS)



Σχήμα 4-10. PDF διάγραμμα χρόνων εξυπηρέτησης στο GPRS (Φορητός Υπολογιστής\GPRS)

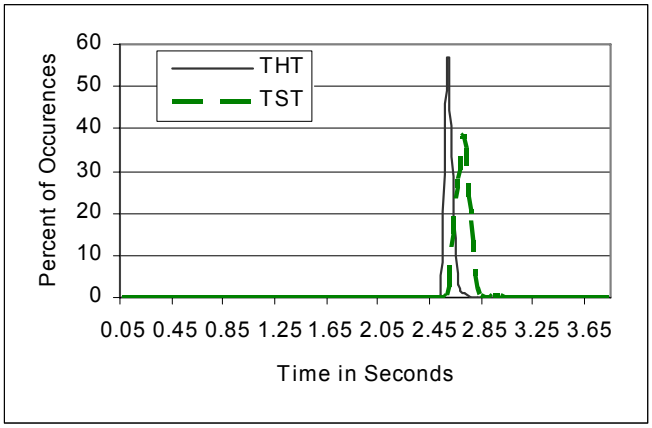
4.4.5. AKA SSL σε Ασύρματο Δίκτυο 802.11b

Προκειμένου να μετρήσουμε το καθαρό (pure) επεξεργαστικό κόστος του AKA SSL μηχανισμού, χρησιμοποιήσαμε την τοπολογία δικτύου που παρουσιάζεται στο Σχήμα 6-4(b). Η εκτέλεση της διαδικασίας σε ένα τόσο γρήγορο δικτυακό περιβάλλον (10 Mbps), επιφέρει τη σημαντική μείωση των χρόνων του δικτύου, με αποτέλεσμα το υπόλοιπο του συνολικού χρόνου να εκφράζει την καθαρή απόδοση του μηχανισμού AKA SSL. Τα αποτελέσματα παρουσιάζονται στον πίνακα 4-4 και στο σχήμα 4-11.

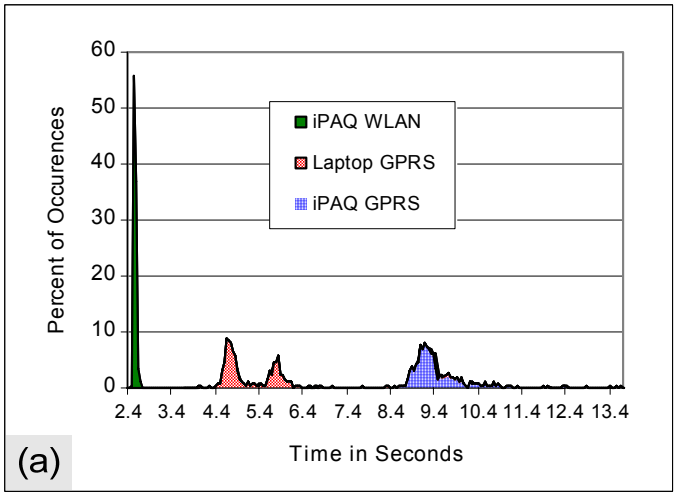
Ο μέσος TST χρόνος είναι πολύ κοντά στον αντίστοιχο THT. Αυτό δικαιολογείται από το γεγονός ότι το NRT είναι αμελητέο και η διακύμανση όλων των τιμών παραμένει πολύ μικρή. Σημειώνεται επίσης ότι ο μέσος THT χρόνος για το iPAQ σε GPRS δίκτυο ήταν 9480 ms. Το ποσό αυτό προσεγγίζεται, προσθέτοντας στα 2605 ms του τρέχοντος πειράματος το χρόνο που απαιτείται για τα round-trips στο GPRS δίκτυο (7 sec). Επίσης, το σχήμα 4-12 παρουσιάζει μια συγκριτική εικόνα των μέσων THT χρόνων για τα τρία σενάρια που υλοποιήσαμε.

	UE (Φορητός Υπολογιστής) (ms)				*Εξυπηρέτης (ms)*
	NRT	RPT	THT	TST	SCRT
M.O. (Average)	103	467	2605	2730	2600
Διακύμανση (S.D.)	377	459	370	376	161

Πίνακας 4-4. Χρόνοι εξυπηρέτησης σε WLAN (iPAQ\WLAN)



Σχήμα 4-11. PDF διάγραμμα χρόνων εξυπηρέτησης (TST & THT) σε WLAN (Φορητός iPAQ\GPRS)



Σχήμα 4-12. Συγκριτικό PDF διάγραμμα των μέσων THT χρόνων

4.5. Μετρήσεις κατανάλωσης Ενέργειας

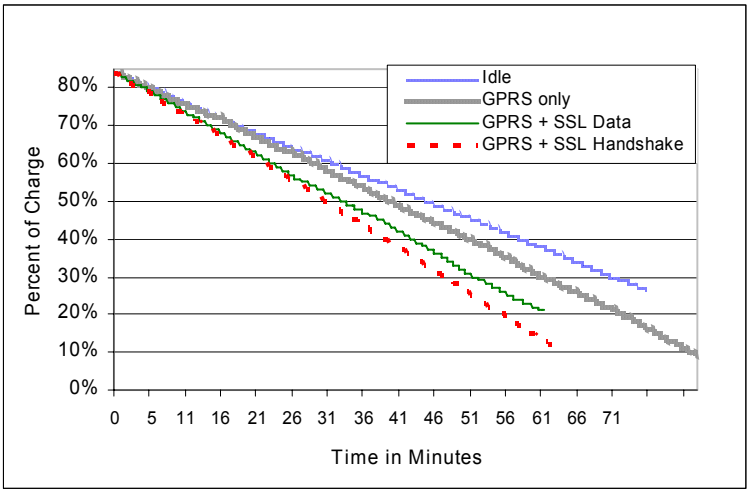
Η ενέργεια που καταναλώνεται από τις φορητές συσκευές κατά τη διάρκεια ασφαλών ασύρματων συνδέσεων μπορεί να ενταχθεί σε δύο μεγάλες κατηγορίες. Η πρώτη περιλαμβάνει τους κρυπτογραφικούς υπολογισμούς που απαιτούνται για την εγκαθίδρυση (establishment)

μιας συνόδου, ενώ η δεύτερη τις ανταλλαγές δεδομένων και μηνυμάτων κατά τη διάρκεια της ίδιας της συνόδου. Σχετικές εργασίες (Karri & Mishra, 2002), οι οποίες διεξήχθησαν με PPC σε δίκτυο τεχνολογίας WLAN 802.11b και WTLS με πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman, έδειξαν κατανάλωση 1062 mJ (milli Joules), εκ των οποίων το 7% καταναλώθηκε σε κρυπτογραφικούς υπολογισμούς και 93% σε ανταλλαγές μηνυμάτων. Μια εκτενής ανάλυση των ενεργειακών απαιτήσεων του πρωτοκόλλου SSL, με τη χρήση του πακέτου OpenSSL και φορητή συσκευή iPAQ, μπορεί να βρεθεί στο (Nachiketh et al., 2003).

Οι προαναφερόμενες εργασίες καλύπτουν σε πολύ μεγάλο βαθμό το ζήτημα κατανάλωσης ενέργειας από το πρωτόκολλο SSL. Η συμβολή της παρούσας διατριβής περιορίζεται στο να μετρήσει την κατανάλωση ενέργειας στις ακόλουθες περιπτώσεις: (α) Η φορητή συσκευή (PPC) βρίσκεται σε κατάσταση αδράνειας (idle) (β) Η συσκευή είναι συνδεδεμένη στο GPRS χωρίς να εκτελεί κάποια συναλλαγή (γ) Η συσκευή είναι συνδεδεμένη στο GPRS και εκτελεί μια SSL χειραψία κάθε 10 δευτερόλεπτα και (δ) η συσκευή είναι συνδεδεμένη στο GPRS και βρίσκεται σε κατάσταση SSL συνόδου, στέλνοντας και λαμβάνοντας συνεχώς δεδομένα μεγέθους 10 KB.

Το iPAQ διαθέτει μια επαναφορτιζόμενη μπαταρία λιθίου (lithium-polymer) χωρητικότητας 400 mAh. Το εξάρτημα επέκτασης (expansion pack), στο οποίο είναι τοποθετημένη η κάρτα D211, διαθέτει μια επιπλέον αποσπώμενη μπαταρία. Η μπαταρία αυτή είχε αφαιρεθεί κατά τη διάρκεια των πειραμάτων μας. Σε όλα τα παραπάνω σενάρια η οθόνη του iPAQ ήταν συνεχώς αναμμένη, ενώ το αρχικό ποσοστό φόρτισης της μπαταρίας ήταν 80%. Η κατανάλωση ενέργειας από τη D211 κάρτα, όταν αυτή είναι συνδεδεμένη σε GPRS, είναι 23 mAh (σε αδράνεια) και 150-200 mAh (εκπομπή – λήψη) αντίστοιχα.

Τα αποτελέσματα των μετρήσεων, τα οποία παρουσιάζονται στο σχήμα 4-13, δείχνουν ότι το iPAQ μπορεί να διατηρεί μια SSL σύνδεση εκπέμποντας και λαμβάνοντας κρυπτογραφημένα δεδομένα για περισσότερο από 2 ώρες. Επίσης, μπορεί να είναι συνδεδεμένο στο GPRS δίκτυο για σχεδόν 2.5 ώρες. Σε κάθε περίπτωση, η δυνατότητα που προφέρει το SSL για συμπίεση (compression) των δεδομένων μπορεί να αποδειχθεί πολύτιμη, μιας και η αποσυμπίεση (decompression) είναι πάντα γρηγορότερη και ενεργειακά πιο οικονομική από τη συμπίεση. Τόσο λοιπόν για τη διαδικασία χειραψίας, όσο και για τα ίδια τα μηνύματα, μπορούμε να ενεργοποιήσουμε τη συμπίεση δεδομένων από την πλευρά του εξυπηρέτη και την αποσυμπίεση στην πλευρά του πελάτη, με σκοπό να βελτιστοποιήσουμε την κατανάλωση στη μπαταρία.



Σχήμα 4-13. Κατανάλωση Ενέργειας (iPAQ\GPRS)

4.6. Σύνοψη – Συμπεράσματα

Το μεγαλύτερο μειονέκτημα των 3GPP διαδικασιών αυθεντικοποίησης είναι ότι εξαρτώνται από την υποκείμενη τεχνολογία προσπέλασης και υποδομής δικτύου και γι' αυτό το λόγο δεν μπορούν να προσφέρουν δυναμικούς και ευπροσάρμοστους μηχανισμούς αυθεντικοποίησης και συμφωνίας κλειδιού. Αντίθετα, για τα συστήματα κινητών επικοινωνιών του μέλλοντος, τέτοιου είδους κλιμακούμενες και δυναμικές λύσεις αποτελούν μονόδρομο, προκειμένου να είναι σε θέση να υποστηρίξουν υπηρεσίες ανάλογα με τη ζήτηση (on-demand), all-IP και απ' άκρο σ' άκρο, ενοποιημένες με το Διαδίκτυο και άλλα ετερογενή περιβάλλοντα.

Σ' αυτό το κεφάλαιο, αντιμετωπίσαμε την αυθεντικοποίηση των συνδρομητών ως υπηρεσία. Έτσι, προτείναμε και περιγράψαμε μια διαδικασία αυθεντικοποίησης και συμφωνίας κλειδιού, η οποία βασίζεται στο πρωτόκολλο SSL και μπορεί να εκμεταλλευτεί τις υπάρχουσες υποδομές δημόσιου κλειδιού. Επιπλέον, διερευνήσαμε και αξιολογήσαμε την απόδοση του προτεινόμενου μηχανισμού, ο οποίος είναι ικανός να προστατέψει την ιδιωτικότητα του χρήστη. Προσπαθήσαμε να εκτιμήσουμε το χρόνο που απαιτείται για να ολοκληρωθεί η απαιτητική σε υπολογιστικούς και δικτυακούς πόρους διαδικασία χειραψίας του μηχανισμού, δοκιμάζοντας διαφορετικές τοπολογίες, σενάρια και φορητές συσκευές.

Λαμβάνοντας υπόψη τις υψηλές ταχύτητες δικτύου που ήδη προσφέρουν τα 3G και B3G συστήματα, τις διάφορες βελτιώσεις του πρωτοκόλλου, καθώς και τις ολοένα και εντυπωσιακότερες τεχνολογικές αναβαθμίσεις στο υλικό των φορητών συσκευών, καταλήξαμε στο συμπέρασμα ότι ο προτεινόμενος AKA SSL μηχανισμός, μπορεί να αποτελέσει μια πραγματοποιήσιμη και αξιόπιστη επιλογή. Ταυτόχρονα, είναι σε θέση να προσφέρει υψηλά επίπεδα εμπιστοσύνης και ασφάλειας στους τελικούς χρήστες και σημαντική ευελιξία και εύκολη κλιμάκωση στους 3G και B3G παρόχους.

Κεφάλαιο 5: Αυθεντικοποίηση χρηστών σε ετερογενή δικτυακά περιβάλλοντα WLAN-3G με χρήση τεχνολογίας PKI.

5.1. Εισαγωγή

Στο κοντινό μέλλον αναμένεται σημαντική αύξηση στον αριθμό των χρηστών, οι οποίοι θα χρησιμοποιούν τις κινητές τους συσκευές για ευαίσθητες, από την πλευρά της ασφάλειας, υπηρεσίες (άμεσης πρόσβασης τραπεζικές υπηρεσίες, χρηματιστηριακές συναλλαγές, ηλεκτρονικές αγορές κτλ). Επιπλέον, οι χρήστες τέτοιων υπηρεσιών θα πρέπει να είναι ικανοί να χρησιμοποιούν με διαφανή (transparent) τρόπο την πλέον κατάλληλη τεχνολογία δικτύου (2.5G ή 3G συστήματα τηλεπικοινωνιών, όπως το GPRS και το UMTS, ευρυζωνικά (broadband) ασύρματα δίκτυα, όπως τα IEEE 802.11 και το High Performance Radio LAN (HiPERLAN) και ασύρματες εκπομπές, όπως το DVB-T), με βάση διάφορα κριτήρια, όπως ο περιβάλλων χώρος (σπίτι, αυτοκίνητο, γραφείο), το κόστος, το προσφερόμενο εύρος δικτύου (bandwidth) κ.ά.

Όπως είδαμε στα προηγούμενα κεφάλαια, η εισαγωγή της τεχνολογίας PKI στα δίκτυα 3G, μπορεί να προσφέρει ισχυρές, ευέλικτες και κλιμακούμενες λύσεις ασφαλείας. Σ' αυτό το πλαίσιο, το πρωτόκολλο SSL/TLS μπορεί να αποτελέσει μια αξιόπιστη και εφικτή εναλλακτική λύση για την παροχή υπηρεσιών αυθεντικοποίησης στους χρήστες των δικτύων αυτών.

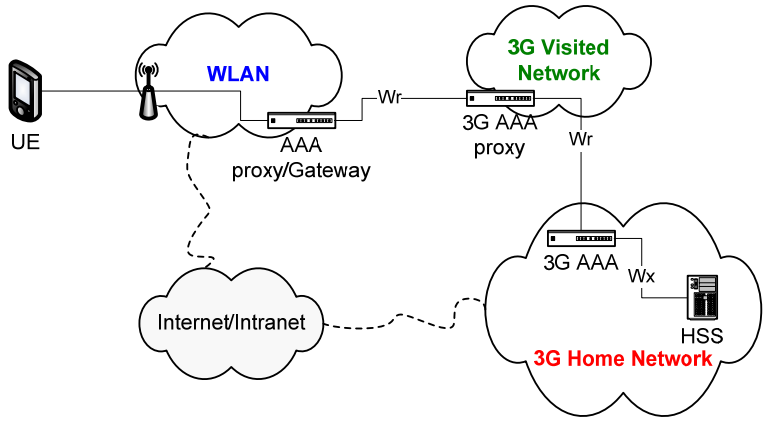
Το παρόν κεφάλαιο, εξετάζει αν το πρωτόκολλο SSL/TLS μπορεί να προσφέρει αξιόπιστες και απ' άκρο σ' άκρο υπηρεσίες αυθεντικοποίησης των χρηστών που κινούνται σε ενοποιημένα περιβάλλοντα 3G και WLAN δικτύων. Ο προτεινόμενος μηχανισμός (Kambourakis et al., 2004e; Kambourakis et al., 2004f) επιτρέπει σε ένα WLAN χρήστη, που είναι ταυτόχρονα συνδρομητής σε κάποιο δίκτυο 3G, να κινείται μεταξύ διαφορετικών WLAN τομέων (domains), οι οποίοι ανήκουν σε διαφορετικούς WLAN παρόχους. Από τεχνολογική άποψη, ο γενικός αυτός μηχανισμός αυθεντικοποίησης, γνωστός με το όνομα Extensible Authentication Protocol (EAP)-TLS, απαιτεί η WLAN αρχιτεκτονική δικτύου να είναι *σφικτά* (tightly) ή *χαλαρά* (loosely) ενσωματωμένη στη 3G αρχιτεκτονική (Salkintzis et al., 2002), ενώ από επιχειρηματική άποψη απαιτούνται ανάλογες συμφωνίες περιαγωγής (roaming agreements) μεταξύ του 3G HN και των αντίστοιχων WLAN παρόχων.

5.2. Ενοποίηση 3G και WLAN Δικτύων

Η σχεδίαση αρχιτεκτονικών B3G βασίζεται στην ιδέα ανάπτυξης ενός κεντρικού (core) IP δικτύου, ενώ το δίκτυο πρόσβασης μπορεί να αποτελείται από μια ποικιλία ετερογενών α-σύρματων τεχνολογιών ανάλογα με την τεχνολογία των κελιών προσπέλασης (access cell). Εστιάζοντας σε περιβάλλοντα μικρο-κελιών (picocells), τα δίκτυα WLAN αποτελούν την πλέον υποσχόμενη τεχνολογία πρόσβασης, παρέχοντας περιορισμένη κάλυψη εντός κτιρίων με μικρό κόστος. Η πολλά υποσχόμενη παροχή μεγάλου πλήθους, αλλά χωρίς κεντρικό συ-ντονισμό μικρο-κελιών, θα φέρει στο προσκήνιο πολλά ανοιχτά ζητήματα σχετικά με την ασφάλεια, την κινητικότητα (mobility), την περιαγωγή και τη χρέωση των χρηστών, οι οποίοι κινούνται μεταξύ διαφορετικών WLAN δικτύων.

Σ' αυτό το κεφάλαιο, εξετάζουμε το ζήτημα της αυθεντικοποίησης B3G χρηστών, προτείνο-ντας την εφαρμογή ενός μηχανισμού βασισμένου στο πρωτόκολλο TLS. Υποθέτουμε ότι οι AAA διαδικασίες που αφορούν τους χρήστες ενός τέτοιου περιβάλλοντος, μπορούν να ελέγ-χονται με συγκεντρωτικό (centralized) ή ημι-συγκεντρωτικό (semi-centralized) τρόπο από το 3G δίκτυο, στο οποίο ο καθένας απ' αυτούς είναι συνδρομητής. Σύμφωνα μ' αυτή την προ-σέγγιση, ένας ή περισσότεροι WLAN τομείς μπορούν να θεωρηθούν ως σημεία πρόσβασης σε μια κοινή 3G δικτυακή υποδομή. Ένας Wi-Fi χρήστης χρειάζεται να γνωρίζει μόνο τον HN πάροχο, ο οποίος είναι υπεύθυνος να συνάπτει και να διατηρεί συμφωνίες περιαγωγής με διάφορους WLAN παρόχους. Έτσι, ανάλογα με τη συμφωνία περιαγωγής μεταξύ των δύο παρόχων, ο χρήστης μπορεί να λαμβάνει υπηρεσίες διαδικτύου από το HN (μέσω του Wi-Fi) ή απευθείας από το WLAN δίκτυο, με την προϋπόθεση ότι έχει αυθεντικοποιηθεί επιτυχώς από το HN. Είναι επίσης φανερό ότι προκειμένου ο χρήστης να είναι ικανός να χρησιμοποιή-σει τέτοιου είδους υπηρεσίες, πρέπει να διαθέτει μια διπλής λειτουργίας (dual mode) συσκευ-ή, η οποία υποστηρίζει WLAN και 3G τεχνολογίες, ή η WLAN συσκευή του μπορεί να συν-δεθεί (μέσω Bluetooth, USB, IrDA) με άλλο εξοπλισμό ο οποίος υποστηρίζει 3GPP υπηρεσί-ες.

Οι τρέχουσες 3GPP προδιαγραφές για το UMTS έκδοση 6 (3GPP TS, 2002d, Koien & Haslestad, 2003) περιγράφουν μία αρχιτεκτονική διασύνδεσης μεταξύ 3G και UMTS, στην οποία το 3G HN είναι υπεύθυνο για έλεγχο πρόσβασης. Η αρχιτεκτονική περιλαμβάνει 3GPP proxy AAA εξυπηρέτες, οι οποίοι αναμεταδίδουν (relay) τη σηματοδοσία ελέγχου πρόσβα-σης στον 3GPP AAA εξυπηρέτη του δικτύου στο οποίο ο χρήστης είναι συνδρομητής (βλ. σχήμα 5-1).



Σχήμα 5-1. Ένταξη WLAN δικτύων στην αρχιτεκτονική UMTS έκδοση 6

Ο μηχανισμός αυθεντικοποίησης των χρηστών μπορεί να βασίζεται στην υπάρχουσα UMTS AKA μέθοδο. Βέβαια, μια τέτοια μέθοδος πρέπει να είναι ανεξάρτητη της WLAN τεχνολογίας πρόσβασης και επιπλέον να υποστηρίζεται από ένα καθιερωμένο (standard) μηχανισμό. Έτσι, η 3GPP φαίνεται να επιλέγει το πρωτόκολλο EAP-AKA, που περιγράφεται στα (3GPP TS, 2002d; Koien & Haslestad, 2003; Arkko & Haverinen, 2003). Το EAP είναι ένα γενικό πρωτόκολλο, το οποίο μπορεί να υποστηρίξει πολλαπλούς μηχανισμούς αυθεντικοποίησης πάνω από σημείο-σε-σημείο (point-to-point, PPP) συνδέσεις. Επομένως, το πρωτόκολλο EAP-AKA παρέχει μια μέθοδο για την ανταλλαγή AKA μηνυμάτων αυθεντικοποίησης ενθυλακωμένων μέσα σε μηνύματα EAP.

Στη περίπτωση που το SN είναι ένα WLAN, η συσκευή του χρήστη συνδέεται σε ένα AP. Ο χρήστης παρουσιάζει το αναγνωριστικό πρόσβασης δικτύου (Network Access Identifier, NAI) (Aboba & Beadles, 1999) που διαθέτει και είναι της μορφής *IMSI@domain* ή *P-TMSI@domain*. Κατόπιν, η αίτηση πρόσβασης προωθείται στον κατάλληλο 3GPP AAA proxy εξυπηρέτη, ο οποίος μεταφράζει την AAA αίτηση στο αντίστοιχο 3G AAA πρωτόκολλο. Η αναζήτηση του proxy εξυπηρέτη βασίζεται στο πεδίο “domain” του NAI και μπορεί να εκτελείται δυναμικά (dynamically searched) ή να είναι διαμορφωμένη εκ των προτέρων (pre-configured). Η σχετική διαδικασία μπορεί να διασχίσει αρκετούς άλλους δικτυακούς τομείς.

Συνήθως, ο EAP εξυπηρέτης είναι διαφορετικός από τον κόμβο αυθεντικοποίησης, ο οποίος βρίσκεται στην περιοχή που κινείται ο χρήστης και μπορεί να είναι, για παράδειγμα, ένα AP ή μια 802.1X γέφυρα (bridge). Η συσκευή του χρήστη, η οποία σ΄ αυτή την περίπτωση είναι γνωστή ως supplicant, επικοινωνεί με τον 3GPP AAA εξυπηρέτη χρησιμοποιώντας γνωστά πρωτόκολλα, όπως το RADIUS (Rigney et al., 2000) και το Diameter (Calhoun et al., 2003). Μια άλλη εργασία, που προτείνει μια νέα μέθοδο αυθεντικοποίησης και συνδυάζει το AAA πλαίσιο με τα χαρακτηριστικά ασφάλειας του UMTS, είναι δυνατό να βρεθεί στο (Hahnsang & Hossam, 2003).

Η παραπάνω προσέγγιση έχει το πλεονέκτημα ότι η διαχείριση της κινητικότητας των χρηστών, η περιαγωγή των συνδέσεων και η χρέωση των συνδρομητών εποπτεύονται από το «κύριο» (master) 3GPP δίκτυο. Κατά συνέπεια, οι χρήστες χρειάζεται να γνωρίζουν μόνο τον 3G πάροχο, ο οποίος είναι υπεύθυνος για τη σύναψη και διατήρηση συμφωνιών περιαγωγής με αντίστοιχους συνεργαζόμενους μ' αυτόν WLAN παρόχους. Επίσης, η λύση αυτή ελαχιστοποιεί τις απαιτούμενες αλλαγές στα κεντρικά δίκτυα των 3GPP παρόχων (π.χ. στα HSS, GGSN).

Από την πλευρά του τελικού χρήστη, ο βασισμένος στη USIM μηχανισμός αυθεντικοποίησης προσφέρει δυο σημαντικά πλεονεκτήματα: (α) Εύκολη ενσωμάτωση των διαπιστευτηρίων (credentials) των WLAN συνδρομητών σ' αυτά του 3G HSS (ίδιος τύπος) (β) Το επίπεδο ασφαλείας του WLAN εξισώνεται με αυτό που προσφέρουν τα 3GPP δίκτυα, επιλύοντας κατά κάποιο τρόπο τις αδυναμίες που εμφανίζονται στα τρέχοντα IEEE 802.11 πρωτόκολλα (Gast, 2002; Eaton, 2003; Peikari & Fogie, 2003).

Παρόλα αυτά, όπως είδαμε προηγουμένως, το πρωτόκολλο EAP-AKA βασίζεται στην ύπαρξη ενός μακροχρόνιου (long-term) συμμετρικού μυστικού κλειδιού για κάθε 3GPP συνδρομητή, ώστε να επιτύχει αμοιβαία αυθεντικοποίηση χρηστών – δικτύου. Αντ' αυτού, θα ήταν περισσότερο αποτελεσματικό να υπήρχε ένας μηχανισμός για τη δυναμική δημιουργία κλειδιού συνόδου. Εισάγοντας το πρωτόκολλο TLS μπορούμε να εκμεταλλευτούμε την προστατευμένη και ευέλικτη διαδικασία διαπραγμάτευσης της σουίτας κρυπτογράφησης, την αμοιβαία αυθεντικοποίηση των επικοινωνουσών οντοτήτων και την κλιμακούμενη διαχείριση των κλειδιών. Έτσι, μπορούμε να παρέχουμε περισσότερο αξιόπιστες διαδικασίες αυθεντικοποίησης και ασφάλεια απ' άκρο σ' άκρο στους χρήστες τέτοιων ετερογενών αρχιτεκτονικών.

5.3. Περιορισμοί και Προβλήματα του μηχανισμού EAP-AKA

Οι περιορισμοί και οι αδυναμίες του πρωτοκόλλου 3GPP AKA, οι οποίες, όπως είναι φυσικό, επηρεάζουν και το πρωτόκολλο EAP-AKA, αναπτύχθηκαν στα σημεία 1-5 της ενότητας 4.3.1. Ακολούθως, παρουσιάζονται ορισμένες αδυναμίες που αφορούν αποκλειστικά το πρωτόκολλο EAP-AKA:

- Η διαδικασία αυθεντικοποίησης είναι πιθανό να απαιτεί την ανταλλαγή αρκετών μηνυμάτων αίτησης / απόκρισης (request / response). Όταν λοιπόν ο χρήστης περιάγει από το ένα κελί στο άλλο, θα πρέπει να αυθεντικοποιείται εκ νέου από τον 3GPP AAA εξυπηρέτη του HN. Κατά συνέπεια, η αποδοτικότητα της διαδικασίας αυθεντικοποίησης εξαρτάται σε σημαντικό βαθμό από την ποιότητα της διαδικασίας μεταβίβασης συνόδων (handover) μεταξύ των εμπλεκόμενων δια-δικτυακών συστημάτων ή τομέων.

- Το πρωτόκολλο EAP-AKA παρέχει προαιρετική υποστήριξη για την προστασία της ιδιωτικότητας του συνδρομητή από παθητικού τύπου επιθέσεις. Όμως, ο συγκεκριμένος μηχανισμός δεν μπορεί να χρησιμοποιηθεί κάθε φορά που ο συνδρομητής συνδέεται σε ένα νέο δικτυακό τομέα. Σ' αυτή την περίπτωση το IMSI του χρήστη στέλνεται σε μορφή καθαρού κειμένου (clear-text).
- Ενεργητικού τύπου επιθέσεις, κατά τις οποίες ο επιτιθέμενος υποδύεται (impersonate) το δίκτυο με στόχο να υποκλέψει το IMSI του συνδρομητή, είναι δυνατό να πραγματοποιηθούν, χρησιμοποιώντας το χαρακτηριστικό (attribute) AT_PERMANENT ID_REQ.
- Το πρωτόκολλο EAP-AKA δε διαθέτει κάποια διαδικασία διαπραγμάτευσης για τον καθορισμό της κρυπτογραφικής σουίτας που θα χρησιμοποιηθεί κατά τη διάρκεια μιας συνόδου.
- Άλλες γνωστού τύπου επιθέσεις, όπως MITM και negotiation attacks που αφορούν το πρωτόκολλο EAP-AKA, περιγράφονται στο (Arkko & Haverinen, 2003).

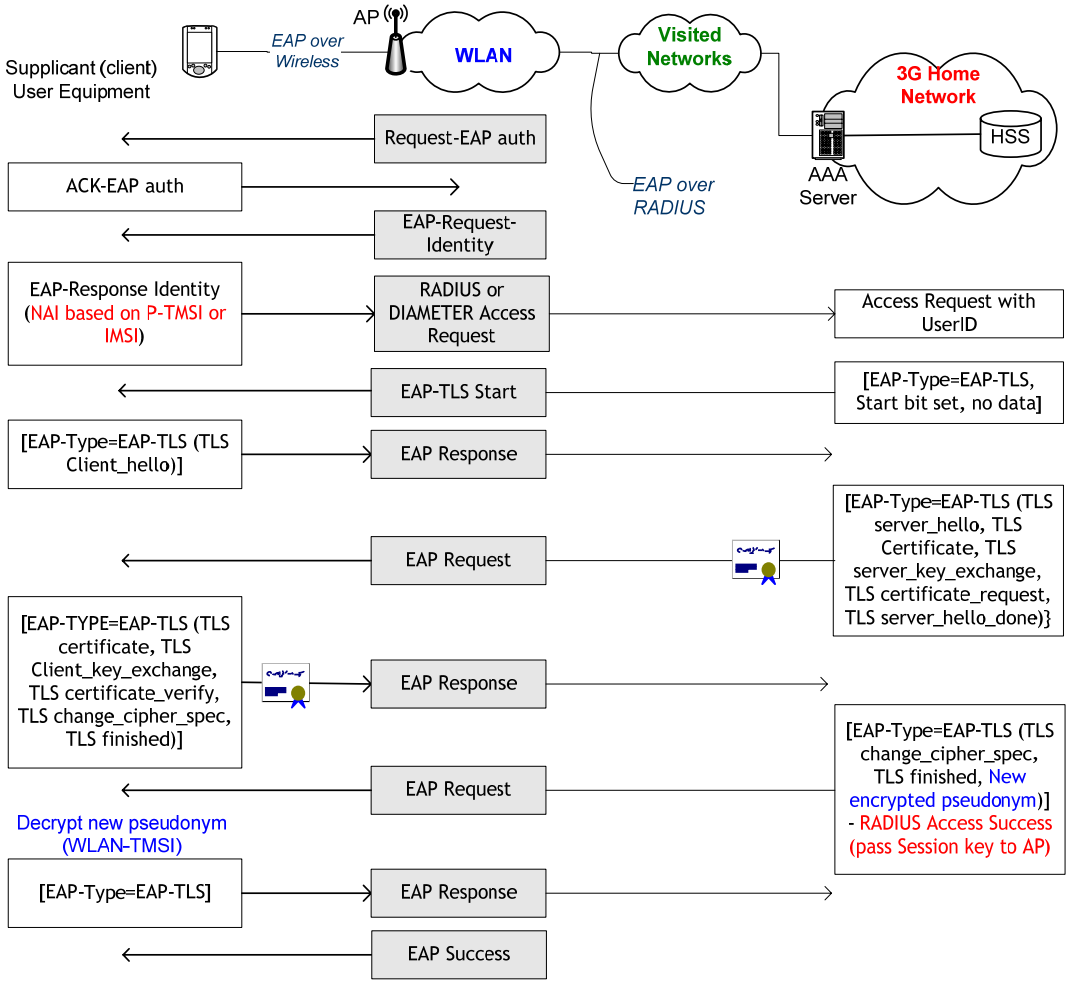
5.4. Μηχανισμός AKA βασισμένος στο πρωτόκολλο EAP-TLS

Το πρωτόκολλο EAP-AKA βασίζεται στην έκδοση 3.0 του πρωτοκόλλου SSL. Ενώ λοιπόν στο Διαδίκτυο το πρωτόκολλο χειραψίας του SSL εκτελείται πάνω από TCP, στο πρωτόκολλο EAP-TLS εκτελείται πάνω από το πρωτόκολλο EAP. Το πρωτόκολλο EAP-TLS υποστηρίζει αμοιβαία αυθεντικοποίηση. Γι' αυτό το λόγο, κάθε πλευρά (supplicant, AAA εξυπηρέτης), πρέπει να αποδείξει στην άλλη την ταυτότητά της, χρησιμοποιώντας το ψηφιακό πιστοποιητικό της και το ιδιωτικό της κλειδί.

Άλλοι μηχανισμοί σχετικοί με το πρωτόκολλο EAP-TLS και κατάλληλοι για ανάπτυξη σε WLAN-3G περιβάλλοντα, είναι τα πρωτόκολλα EAP-Tunneled Transport Layer Security (EAP-TTLS) (Funk & Blake-Wilson, 2002) και Protected EAP (PEAP) (Palekar et al., 2004). Και τα δύο αυτά πρωτόκολλα αναπτύχθηκαν σε απάντηση του PKI περιορισμού που απαιτείται από το πρωτόκολλο EAP-TLS και κατά συνέπεια χρησιμοποιούν άλλες μεθόδους αυθεντικοποίησης των χρηστών, οι οποίες δεν βασίζονται σε PKCs. Είναι χαρακτηριστικό ότι το πρωτόκολλο TTLS απασχόλησε πρόσφατα τη 3GPP προκειμένου να χρησιμοποιηθεί σε ετερογενή περιβάλλοντα 3G-WLAN, αλλά όπως περιγράφεται στο (Asokan et al., 2002) ήταν ευάλωτο σε επιθέσεις του τύπου MITM. Ο οργανισμός προτυποποίησης 3GPP2 έχει επίσης συμφωνήσει να υιοθετήσει το πρωτόκολλο TLS σε συνδυασμό με συμμετρικά κλειδιά ως μια από τις μεθόδους αυθεντικοποίησης σε περιβάλλον 3GPP2-WLAN (3GPP TSG, 2004; 3GPP2 TSG, 2004). Ακόμα, η πιθανή χρήση του ίδιου πρωτοκόλλου σε ετερογενή ασύρματα δίκτυα εξετάζεται στο (Chen et al., 2003).

Όπως είδαμε, η χρήση του πρωτοκόλλου EAP-TLS απαιτεί κάποιο είδος υποδομής δημόσιου κλειδιού. Οι προϋποθέσεις και οι μέθοδοι ενσωμάτωσης PKI τεχνολογίας σε υβριδικό περιβάλλον 3G-WLAN παραμένουν ίδιοι με αυτούς που περιγράφηκαν στις ενότητες 2.3.1, 2.3.2 και 4.2.

Υποκινούμενοι λοιπόν από τα πλεονεκτήματα της ενσωμάτωσης τεχνολογίας PKI στα 3G/WLAN δίκτυα και του πρωτοκόλλου SSL, καθώς και από τις σύγχρονες τεχνολογικές εξελίξεις (βλ. ενότητα 4.2), προτείνουμε έναν AKA μηχανισμό για ετερογενή 3G/WLAN περιβάλλοντα, ο οποίος βασίζεται στο πρωτόκολλο EAP-TLS αντί στο πρωτόκολλο EAP-AKA. Ο προτεινόμενος μηχανισμός παρουσιάζεται στο σχήμα 5-2. Η διαδικασία εστιάζεται στις ανταλλαγές μηνυμάτων μεταξύ των δύο μερών καθώς στις λειτουργίες δημόσιου κλειδιού από την πλευρά του supplicant, ο οποίος διαθέτει περιορισμένους υπολογιστικούς πόρους. Επίσης, το συγκεκριμένο σχήμα ενσωματώνει και μια προστατευόμενη διαδικασία απόδοσης νέου P-TMSI από τον εξυπηρέτη στο supplicant.



Σχήμα 5-2. Μηχανισμός AKA βασισμένος στο πρωτόκολλο EAP-TLS

Η επιλογή του κατάλληλου 3GPP AAA εξυπηρέτη βασίζεται στο NAI που αποστέλλει ο supplicant. Εφόσον λοιπόν ο πελάτης ισχυρίζεται την ταυτότητά του στο μήνυμα EAP-response

identity, ο EAP εξυπηρέτης πρέπει να επαληθεύσει ότι η αυτή αντιστοιχεί στο πιστοποιητικό που ο supplicant θα του παρουσιάσει στο δεύτερο μήνυμα EAP Response. Επομένως, η ταυτότητα του χρήστη πρέπει να περιλαμβάνεται στο πιστοποιητικό που θα αποστείλει στον AAA εξυπηρέτη. Επιπλέον, από την πλευρά του εξυπηρέτη, απαιτείται αντιστοίχιση του P-TMSI στο σωστό IMSI. Με παρόμοιο τρόπο, ο supplicant είναι υποχρεωμένος να ελέγξει αν το πιστοποιητικό του εξυπηρέτη είναι έγκυρο (υπογεγραμμένο από έμπιστη CA, χρόνος λήξης, όνομα οντότητας που πιστοποιεί κτλ). Το πρωτόκολλο EAP-TLS περιγράφεται αναλυτικά στο (Aboba and Simon, 1999).

Συγκρίνοντας τις δύο μεθόδους (EAP-AKA και EAP-TLS) διαπιστώνουμε τα παρακάτω:

- Η 3GPP αρχιτεκτονική διασύνδεσης δικτύων 3G και WLAN παραμένει η ίδια με την προσθήκη μιας ή περισσοτέρων PKI, η οποία, όπως είδαμε στην ενότητα 2.3.1, μπορεί να μην αποτελεί τμήμα του κεντρικού δικτύου του 3GPP παρόχου αλλά να συνεργάζεται μ' αυτόν με τη μορφή ενός TTP/CSP.

- Ο supplicant και ο AAA εξυπηρέτης πρέπει να υποστηρίζουν το πρωτόκολλο EAP-TLS, ενώ τα διάφορα APs πρέπει να αναγνωρίζουν την EAP-TLS διαδικασία αυθεντικοποίησης. Σήμερα το πρωτόκολλο EAP-TLS προσφέρεται από τους σημαντικότερους κατασκευαστές δικτυακού εξοπλισμού σε δικτυακές συσκευές, όπως είναι οι δρομολογητές (routers), τα APs και οι κινητές συσκευές των τελικών χρηστών. Αυτό εγγυάται εύκολη ενσωμάτωση στα υπάρχοντα δίκτυα καθώς και ελάχιστες αλλαγές στον ήδη εγκατεστημένο δικτυακό εξοπλισμό.

- Οποιοσδήποτε AAA εξυπηρέτης (WLAN ή 3G), ο οποίος βρίσκεται κοντά στον supplicant, μπορεί να παρέχει υπηρεσίες αυθεντικοποίησης, βελτιώνοντας κατ' αυτόν τον τρόπο την κινητικότητα (mobility). Αυτό είναι δυνατό μιας και ο συγκεκριμένος AAA εξυπηρέτης μπορεί να αλληλο-πιστοποιηθεί (cross-certification) με τον AAA εξυπηρέτη του 3GPP HN. Εναλλακτικά, μπορεί και οι δύο να διαθέτουν πιστοποιητικά υπογεγραμμένα από έναν κοινό CSP. Η συγκεκριμένη δυνατότητα χρήζει ιδιαίτερης προσοχής, αφού το UE δε διαθέτει σύνδεση στο WLAN πριν ολοκληρωθεί επιτυχώς η διαδικασία αυθεντικοποίησης. Παρόλα αυτά, δεδομένου ότι το πλήθος των CAs θα τείνει ολοένα αυξανόμενο, η πιθανότητα για το UE να λάβει μια αλυσίδα πιστοποιητικών με άγνωστη αγκύρωση (anchor) μεγαλώνει. Σ' αυτή την περίπτωση, το UE μπορεί να εκμεταλλευτεί το γεγονός ότι διαθέτει μόνιμη σύνδεση με το 3GPP δίκτυο (always-on ability). Με άλλα λόγια, μπορεί να επιστρέψει (switch) άμεσα στο UMTS δίκτυο και να επαληθεύσει το πιστοποιητικό του άγνωστου AAA εξυπηρέτη.

- Η διαδικασία ανάκλησης (revocation) των πιστοποιητικών του supplicant μπορεί να βασίζεται στο IMSI, αποφεύγοντας έτσι τη δημιουργία και διανομή CRLs (βλ. ενότητα 4.4.1).

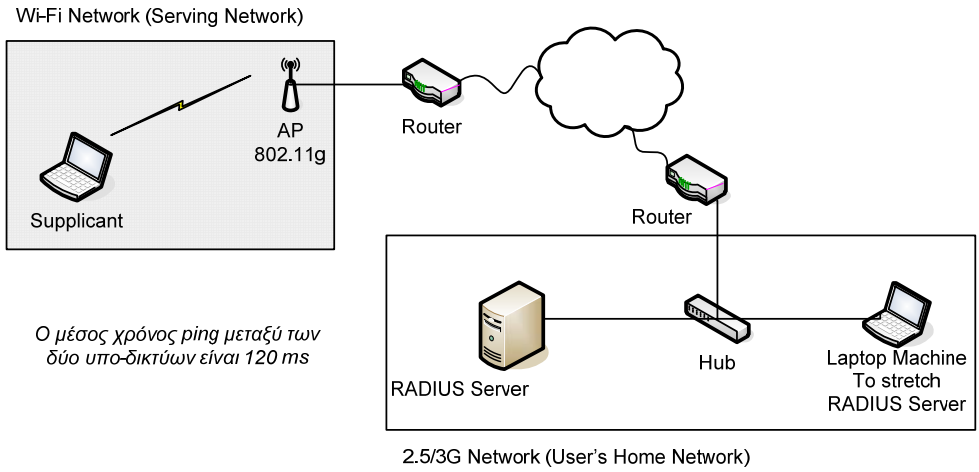
- Η συνολική απόδοση του EAP-TLS μηχανισμού μπορεί να βελτιωθεί σημαντικά, χρησιμοποιώντας τη δυνατότητα του TLS πρωτοκόλλου για ανανέωση συνδέσεων (βλ. ενότητα 4.3.3). Ο σκοπός για τον οποίο το session ID περικλείεται στο μήνυμα *Hello* του supplicant είναι να επιτρέψει την ανανέωση της συγκεκριμένης συνόδου, βελτιστοποιώντας τη συνολική απόδοση του πρωτοκόλλου χειραψίας. Αυτό είναι ιδιαίτερα εξυπηρετικό στην περίπτωση που ο supplicant επιχειρεί επανειλημμένα, μέσα σε σύντομο χρονικό διάστημα να συνδεθεί στον ίδιο AAA εξυπηρέτη. Ανάλογα με το session ID που επιθυμεί να ανανεώσει ο πελάτης και το χρονικό διάστημα που μεσολάβησε από την προηγούμενη διαδικασία αυθεντικοποίησης, ο EAP εξυπηρέτης θα αποφασίσει αν η προτεινόμενη σύνοδος μπορεί να ανανεωθεί ή όχι. Επίσης, όπως είδαμε στις ενότητες 4.2 και 4.4.2, η συνολική απόδοση του πρωτοκόλλου χειραψίας του SSL/TLS μπορεί να βελτιωθεί σημαντικά.
- Το πρωτόκολλο SSL/TLS έχει αποδείξει την αποτελεσματικότητά του στο ενσύρματο Διαδίκτυο και υποστηριζόμενο από τεχνολογία PKI είναι το πλέον κατάλληλο για να υποστηρίξει μεγάλης κλίμακας ετερογενείς αρχιτεκτονικές. Η ευελιξία επιλογής αρκετών διαφορετικών σουιτών κρυπτογράφησης αμβλύνει την πιθανότητα επιθέσεων.
- Η εφαρμογή του μηχανισμού EAP-TLS καταργεί την ανάγκη για δημιουργία και διανομή διανυσμάτων αυθεντικοποίησης από το HSS, απομακρύνοντας έτσι τον ορατό κίνδυνο κλοπής ή καταστροφής τους. Από την άλλη πλευρά, η αμοιβαία διαδικασία αυθεντικοποίησης ελέγχεται από τα ψηφιακά πιστοποιητικά που διαθέτουν τα δύο μέρη.
- Το πρωτόκολλο EAP-TLS παρέχει υπηρεσίες αυθεντικοποίησης απ' άκρο σ' άκρο, σε αντίθεση με το EAP-AKA, το οποίο παρέχει υπηρεσίες ασφαλείας του τύπου από κόμβο σε κόμβο (*hop-by-hop*). Αυτό συμβαίνει διότι οι ενδιάμεσοι κόμβοι πρέπει να υποστηρίζουν πρωτόκολλα, όπως το IPsec, το MAPsec ή το SSL/TLS για την εξασφάλιση των διαδικτυακών επικοινωνιών.

5.5. Εκτίμηση της απόδοσης του μηχανισμού EAP-TLS

5.5.1. Περιγραφή της διαδικασίας

Προκειμένου να εκτιμήσουμε την απόδοση του μηχανισμού EAP-TLS σε χρόνους εξυπηρέτησης, χρησιμοποιήσαμε την τοπολογία που παρουσιάζεται στο σχήμα 5-3. Ο κινητός εξοπλισμός του χρήστη αποτελείται από ένα φορητό υπολογιστή (laptop), ο οποίος χρησιμοποιεί επεξεργαστή τύπου Pentium II χρονισμένο στα 400 MHz και διαθέτει 80 MB κύριας μνήμης την οποία διαχειρίζεται το λειτουργικό σύστημα Windows XP. Από την άλλη πλευρά, ο RADIUS εξυπηρέτης είναι εγκατεστημένος σε μια μηχανή με επεξεργαστή Pentium 4 χρονισμένο στα 1.4 MHz και ενσωματώνει 128 MB κύριας μνήμης, την οποία διαχειρίζεται το λειτουργικό σύστημα Linux Slackware στην έκδοση 9.1 (www.slackware.com). Επίσης, στον

εξυπηρέτη εγκαταστάθηκε και παραμετροποιήθηκε το πακέτο λογισμικού ανοικτού κώδικα Freeradius (www.freeradius.org) στην έκδοση 0.9.3.



Σχήμα 5-3. Η τοπολογία που αξιοποιήθηκε

Ο πελάτης συνδέεται στο ασύρματο δίκτυο χρησιμοποιώντας μια IEEE 802.11g PCMCIA κάρτα και ένα IEEE 802.11g AP. Ο RADIUS εξυπηρέτης είναι εγκατεστημένος σε διαφορετικό υπο-δίκτυο από αυτό που βρίσκεται το AP. Ο μέσος χρόνος ping μεταξύ των δύο αυτών δικτύων μετρήθηκε περίπου στα 120 ms. Στο ίδιο υπο-δίκτυο με τον RADIUS εξυπηρέτη τοποθετήσαμε έναν ακόμη φορητό υπολογιστή, ο οποίος είχε ως αποστολή να παράγει ένα μεγάλο πλήθος EAP-TLS αιτήσεων, δημιουργώντας σημαντικό υπολογιστικό φόρτο στον εξυπηρέτη. Ο χρόνος μεταξύ διαδοχικών EAP-TLS αιτήσεων αυθεντικοποίησης ακολουθεί την αρνητικά εκθετική κατανομή (negative exponential distribution). Επίσης, τα απαραίτητα ψηφιακά πιστοποιητικά για τα πειράματά μας δημιουργήθηκαν με το πακέτο ανοικτού κώδικα OpenSSL στην έκδοση 0.9.7c.

Η διαδικασία αυθεντικοποίησης είναι αμοιβαία. Οι δύο πλευρές ανταλλάσσουν πιστοποιητικά, τα οποία διατηρούνται τοπικά μαζί με τα δημόσια κλειδιά των έμπιστων CAs. Επίσης για να μελετήσουμε ένα σενάριο αυθεντικοποίησης σε SN χρησιμοποιήσαμε αλυσίδα πιστοποιητικών βάθους 2. Και τα δύο μέρη ελέγχουν την εγκυρότητα των πιστοποιητικών που λαμβάνουν (χρόνος λήξης, αγκύρωση (trust anchor), ψηφιακή υπογραφή). Αντίθετα, δεν εκτελείται κάποιος έλεγχος για ανακληθέντα πιστοποιητικά. Μόνον ο RADIUS εξυπηρέτης είναι υποχρεωμένος να κάνει κάτι τέτοιο, συγκρίνοντας το P-TMSI του supplicant, που προσδιορίζεται στο NAI, με το αντίστοιχο IMSI.

5.5.2. Αποτελέσματα Μετρήσεων

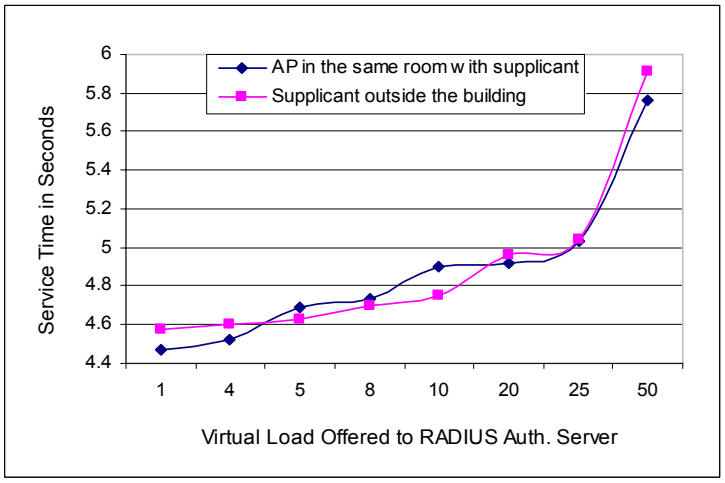
Κατά τη διάρκεια των υπολογισμών, χρησιμοποιήσαμε διάφορες τιμές της παραμέτρου λ η οποία ρυθμίζει το ρυθμό άφιξης των αιτήσεων, για τη διεργασία που δημιουργεί εικονικό φόρτο στον RADIUS εξυπηρέτη. Καταγράψαμε 1000 μετρήσεις από ίσο αριθμό συναλλαγών

οι οποίες εκκινήθηκαν από τον supplicant. Για τη συλλογή των μετρήσεων χρησιμοποιήσαμε το εργαλείο ανάλυσης της κίνησης ethernet δικτύων Ethereal (www.ethereal.com) στην έκδοση 0.10.0, καθώς και τα αντίστοιχα αρχεία καταγραφής (log files) του RADIUS εξυπηρέτη. Ο μέσος χρόνος αρχικοποίησης για τον supplicant ήταν 0.062 sec. Οι μέσες τιμές των EAP-TLS χρόνων εξυπηρέτησης για τα διάφορα σενάρια που υλοποιήσαμε, παρουσιάζονται στον πίνακα 5-1, ενώ στο σχήμα 5-4 δίνεται μια γραφική αναπαράστασή τους.

Εικονικός φόρτος (λ)	*Το AP βρίσκεται στον ίδιο χώρο με τον supplicant*	*Ο supplicant κινείται εκτός κτιρίου στο οποίο είναι εγκατεστημένο το AP*
1	4.468	4.575
4	4.524	4.604
5	4.694	4.625
8	4.737	4.695
10	4.897	4.753
20	4.917	4.959
25	5.036	5.045
50	5.761	5.912
Μέσος Όρος	4.879	4.896

Πίνακας 5-1. Μέσοι χρόνοι εξυπηρέτησης EAP-TLS αιτήσεων

Οπωσδήποτε ένας μέσος χρόνος αυθεντικοποίησης κάτω από 5 δευτερόλεπτα, όπως αυτός εμφανίζεται στην τελευταία γραμμή του πίνακα 5-1, είναι αποδεκτός από ένα χρήστη υπηρεσιών 3G/B3G, λαμβάνοντας υπόψη και το γεγονός ότι η συνήθης 2.5G AKA διαδικασία σε SN, διαρκεί από 5 έως 7 δευτερόλεπτα. Παρόλα αυτά, ο χρόνος αυτός θα τείνει αυξανόμενος ανάλογα με την απόσταση (μεταφραζόμενη σε χρόνους ping) μεταξύ του SN και του αντίστοιχου HN. Αυτό οφείλεται κυρίως στο σημαντικό αριθμό round-trips που απαιτεί το πρωτόκολλο EAP-TLS. Βέβαια, όπως είδαμε στην ενότητα 4.4.3, η διαδικασία χειραψίας του πρωτοκόλλου SSL/TLS είναι δυνατό να επιταχυνθεί σημαντικά χρησιμοποιώντας τεχνικές ενταμίευσης (buffering), επανάληψη προηγούμενων συνδέσεων (resuming), αλλά και βελτιστοποιημένες κρυπτογραφικές σουίτες.



Σχήμα 5-4. Χρόνοι εξυπηρέτησης EAP-TLS

Είναι επίσης φανερό, ότι η απόσταση μεταξύ του AP και του supplicant ελάχιστα επιδρά στο συνολικό χρόνο εξυπηρέτησης. Ανακαλύψαμε ότι αυτό παραμένει αληθές όσο η ποιότητα του σήματος (signal quality) υπερβαίνει το 55-60%. Επιπλέον, το μέγεθος των πιστοποιητικών όχι μόνο επιβραδύνει τη διαδικασία επαλήθευσής τους στην κάθε πλευρά, αλλά επιπλέον προσθέτει αρκετά bytes στα αντίστοιχα μηνύματα χειραψίας. Επιπλέον επιβάρυνση στο συνολικό χρόνο εξυπηρέτησης αναμένεται να παρατηρηθεί στην περίπτωση που ο RADIUS εξυπηρέτης είναι σημαντικά απομακρυσμένος από το HSS του HN. Σ' αυτή την περίπτωση ο RADIUS εξυπηρέτης πρέπει να επικοινωνήσει με το ανάλογο HSS προκειμένου να ανακτήσει τις απαιτούμενες πληροφορίες που περιλαμβάνονται στο προφίλ του χρήστη (π.χ. σχετικά με το τι είναι εξουσιοδοτημένος ο χρήστης να κάνει) και να τον αυθεντικοποιήσει με επιτυχία.

5.7. Σύνοψη – Συμπεράσματα

Ο τομέας των κινητών επικοινωνιών χαρακτηρίζεται από διαρκή ανάπτυξη, πλησιάζοντας όλο και περισσότερο στην προοπτική της all-IP 4^{ης} γενιάς. Σ' αυτό το κεφάλαιο, ασχοληθήκαμε με το πρόβλημα της αυθεντικοποίησης των χρηστών που κινούνται σε ετερογενή 3GPP/WLAN περιβάλλοντα. Υποστηρίξαμε ότι ο μηχανισμός EAP-TLS, υποβοηθούμενος από υποδομές δημόσιου κλειδιού, μπορεί να προσφέρει ευέλικτες, εύκολα κλιμακούμενες και απ' άκρο σ' άκρο λύσεις στο συγκεκριμένο πρόβλημα.

Λαμβάνοντας υπόψη τις τρέχουσες τεχνικές προδιαγραφές της 3GPP στο συγκεκριμένο θέμα, αντιπαραβάλαμε την πρότασή μας με τον προτεινόμενο από αυτήν μηχανισμό EAP-AKA. Συμπεράναμε ότι το πρωτόκολλο EAP-TLS μπορεί να ξεπεράσει τις ανεπάρκειες που παρουσιάζουν οι μηχανισμοί αυθεντικοποίησης των 3GPP και WLAN συστημάτων, ενώ ταυτόχρο-

να απαιτεί ελάχιστες αλλαγές στην 3GPP αρχιτεκτονική και στον εμπλεκόμενο δικτυακό εξοπλισμό.

Προκειμένου να εκτιμήσουμε την απόδοση του προτεινόμενου μηχανισμού σε πραγματικό περιβάλλον, χρησιμοποιήσαμε μια πρότυπη διάταξη και αρκετά διαφορετικά σενάρια. Τα αποτελέσματα, με τη μορφή μέσων χρόνων εξυπηρέτησης, ενισχύουν την άποψη ότι ο μηχανισμός EAP-TLS μπορεί να αποτελέσει μια αξιόπιστη και προπαντός εύκολα προσαρμόσιμη εναλλακτική λύση.

Κεφάλαιο 6: Παροχή ψηφιακών πιστοποιητικών ιδιοτήτων σε χρήστες ετερογενών δικτύων WLAN-3G

6.1. Εισαγωγή

Στο κοντινό μέλλον οι χρήστες των δικτύων κινητών επικοινωνιών θα χρησιμοποιούν συχνά συγκεκριμένες και περιορισμένης διάρκειας υπηρεσίες, όπως η αγορά ενός αγαθού από ένα κατάστημα άμεσης πρόσβασης (on-line), ο διακανονισμός μετοχών με μια τράπεζα ή η προσκόμιση (download) ενός αρχείου από μια προστατευμένη δικτυακή τοποθεσία. Κάτι τέτοιο μπορεί να πραγματοποιηθεί, χρησιμοποιώντας προσωρινά (temporary), μικρής διάρκειας (short-lived) ψηφιακά πιστοποιητικά ιδιοτήτων (Attribute Certificates, AC). Οι αρχές πιστοποίησης ιδιοτήτων (Attribute Authorities, AA) συνδέουν τα χαρακτηριστικά (ή ιδιότητες) μιας οντότητας με την ταυτότητά της, υπογράφοντας το κατάλληλο AC (Farrell & Housley, 2002).

Οι ιδιότητες (attributes) μπορούν να προσδιορίζουν συμμετοχή σε κάποια ομάδα (membership), συγκεκριμένο ρόλο (role), εξουσιοδότηση προσπέλασης ή άλλες πληροφορίες εξουσιοδότησης, οι οποίες συνδέονται με τον κάτοχο του συγκεκριμένου AC. Για τους παραπάνω λόγους, τα ACs είναι ιδιαιτέρως κατάλληλα για την υλοποίηση διαδικασιών εξουσιοδότησης βασισμένων σε ρόλους (role-based), καθώς και έλεγχο προσπέλασης (Oppliger et al, 2000; Farrell & Housley, 2002). Επίσης, χρησιμοποιώντας ACs, μπορούμε να υλοποιήσουμε δημοφιλείς μηχανισμούς εξουσιοδότησης, όπως ο μηχανισμός Role-Based Access Control (RBAC) (Ferraiolo et al, 1995).

Τα ACs θεωρητικά μοιάζουν με τα Privilege Access Certificates (PACs), τα οποία χρησιμοποιούνται στο SESAME και στο λειτουργικό σύστημα Microsoft Windows 2000. Η δυνατότητα χρήσης ACs, έχει συμπεριληφθεί στα πρότυπα ANSI X9.57 και X.509 των οργανισμών ITU-T (ITU-T, 1997) και ISO/IEC, ως ένας εναλλακτικός και καλύτερος τρόπος από αυτόν των PKCs για τη μεταφορά πληροφοριών εξουσιοδότησης. Γνωστά συστήματα γενικής εξουσιοδότησης, τα οποία χρησιμοποιούν ACs είναι τα Akenti (Thompson et al., 1999; http://www.itg.lbl.gov/security/Akenti/homepage.html;) και Permis (Chadwick, 2002; Otenko & Chadwick, 2003). Επίσης, υπηρεσίες εξουσιοδότησης βασισμένες σε ACs αποτελούν επέκταση του γνωστού πρωτοκόλλου TLS. Πρέπει επίσης να σημειωθεί, ότι στη βιβλιογραφία (Arsenault and Turner, 2002) συχνά χρησιμοποιείται ο όρος Privilege Management Infra-

structure (PMI) για να δηλώσει υποδομές που χρησιμοποιούν αποκλειστικά AAs και ACs, αντί του γενικότερου όρου PKI.

Η βασική δομή ενός AC παρουσιάζεται στο σχήμα 6-1. Ένα από τα πλεονεκτήματα αυτών των προσωρινών πιστοποιητικών είναι ότι έχουν μικρή διάρκεια ζωής και γι' αυτό το λόγο, συνήθως, δε χρειάζεται να συμπεριληφθούν σε κάποια CRL. Το ίδιο ισχύει αν έχουν εκδοθεί στα πλαίσια μιας προ-πληρωμένης (pre-paid) υπηρεσίας. Η χρήση ACs μπορεί να υποστηρίξει και υπηρεσίες μη-αποποίησης.

Version (Έκδοση)
Holder (Κάτοχος)
Issuer (Εκδότης)
Signature (Υπογραφή)
Serial Number (Σειριακός αριθμός)
Attribute Certificate Validity Period (Περίοδος ισχύος)
Attributes (Ιδιότητες που πιστοποιούνται)
Issuer Unique ID (Αναγνωριστικό του εκδότη)
Extensions (Επεκτάσεις)

Σχήμα 6-1. Η βασική δομή ενός Πιστοποιητικού Ιδιοτήτων

Ένα διαφορετικό πεδίο εφαρμογής της συγκεκριμένης τεχνολογίας είναι ο φορητός κώδικας (mobile code), ο οποίος τα τελευταία χρόνια χρησιμοποιείται σε διάφορες εφαρμογές των ενσύρματων και ασύρματων δικτύων. Η διαδικασία δημιουργίας φορητού κώδικα απαιτεί τα προγράμματα ή τα τμήματα κώδικα (code segments) να μπορούν να ανταλλάσσονται και να χρησιμοποιούνται μεταξύ ετερογενών συστημάτων ή δικτύων χωρίς να υφίστανται καμία αλλαγή ή προσαρμογή (Oppliger, 2000). Μία λύση για την προστασία του περιβάλλοντος εκτέλεσης (π.χ. φορητή συσκευή) από κακόβουλο (malicious) φορητό κώδικα είναι η αυθεντικοποίησή του πριν αυτός εκτελεστεί. Αυτή η μέθοδος είναι γνωστή ως *Shrink-Wrap*. Έτσι, αν και δεν είναι πάντα δυνατό να αποφασίσουμε αν ένα τμήμα φορητού κώδικα περιέχει κακόβουλες εντολές, μπορούμε τουλάχιστον να τον αυθεντικοποιήσουμε. Αυτή η δυνατότητα μπορεί να αποδειχθεί πολύ χρήσιμη για έναν κατασκευαστή λογισμικού, ο οποίος υπογράφει ψηφιακά το φορητό κώδικά του και τον διανέμει μαζί με το AC, το οποίο απαιτείται για να επαληθευτεί η γνησιότητα του λογισμικού.

Για παράδειγμα, υποθέτουμε ότι ένας χρήστης φορητής συσκευής Palm συνδέεται μέσω GPRS σε κάποια δικτυακή πύλη (mobile portal) και αναζητά λογισμικό παιχνιδιών. Αυτό που ασφαλώς χρειάζεται να γνωρίζει είναι αν το παιχνίδι που διάλεξε είναι τουλάχιστον αυθεντικό. Από την άλλη πλευρά, ένας προγραμματιστής, ο οποίος δημιουργεί εφαρμογές για συγκεκριμένες φορητές συσκευές, επιθυμεί να υπογράψει ψηφιακά τον κώδικά του και να τον το-

ποθετήσει μαζί με το αντίστοιχο ψηφιακό πιστοποιητικό σε κάποια δικτυακή πύλη. Γι' αυτό το σκοπό χρειάζεται να αποκτήσει ένα AC. Σε ένα παρόμοιο περιβάλλον υποθέτουμε ότι είναι δυνατό να υπάρχουν πολλές AAs, οι οποίες μπορούν να εκδίδουν τέτοιου είδους πιστοποιητικά σε συνεργασία με τους παρόχους των αντίστοιχων υπηρεσιών. Αν, για παράδειγμα, ένας οργανισμός χρησιμοποιεί κάποιο είδος PKI για τη διανομή PKCs και άλλων σχετικών υπηρεσιών, τότε το ίδιο μπορεί να χρησιμοποιηθεί για την έκδοση και τη διανομή ACs.

Λαμβάνοντας υπόψη τις τρέχουσες τεχνικές προδιαγραφές της 3GPP για ενοποιημένα WLAN-3G περιβάλλοντα (3GPP TS, 2004; 3GPP TS, 2004b; 3GPP TS, 2004c; Koien & Haslestad, 2003; Salkintzis et al., 2002), το παρόν κεφάλαιο προτείνει μια υβριδική αρχιτεκτονική WLAN-3G, η οποία είναι ικανή να υποστηρίξει υπηρεσίες σχετικές με την έκδοση και διανομή ACs. Αν και η 3GPP δεν υποθέτει κάποιο συγκεκριμένο τύπο δικτύων WLAN, για τις ανάγκες της ανάλυσης που θα ακολουθήσει υποθέτουμε ότι αυτός είναι ο IEEE 802.11. Η προτεινόμενη αρχιτεκτονική επιτρέπει σε ένα Wi-Fi χρήστη, ο οποίος είναι ταυτόχρονα συνδρομητής σε κάποιο 3GPP δίκτυο, να μετακινείται μεταξύ διαφορετικών WLAN τομέων και να αποκτά ACs ανάλογα με τις ανάγκες του. Ως αποτέλεσμα, ο χρήστης χρειάζεται να γνωρίζει μόνο τον HN 3GPP πάροχο, ο οποίος είναι υπεύθυνος να συνάπτει και να διαχειρίζεται συμφωνίες περιαγωγής με ενδιάμεσους ή τελικούς 3GPP και WLAN παρόχους.

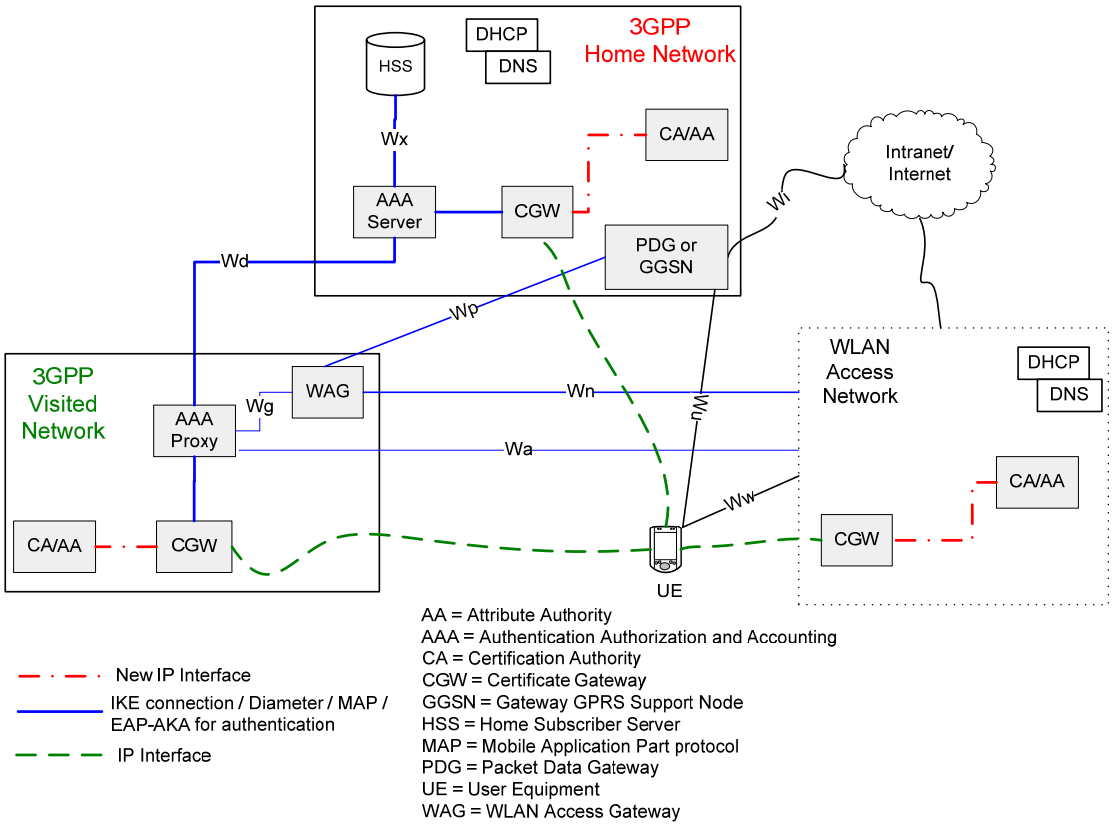
6.2. Η προτεινόμενη Αρχιτεκτονική

Πολύ πρόσφατες τεχνικές προδιαγραφές της 3GPP για το σύστημα UMTS έκδοση 6, (3GPP TS, 2004d; 3GPP TS, 2003c) διερευνούν την πιθανότητα ανάπτυξης τεχνολογίας PKI στα δίκτυα των 3G παρόχων, για την υποστήριξη υπηρεσιών έκδοσης και χρήσης ψηφιακών πιστοποιητικών από τους συνδρομητές. Παρόλα αυτά, η προσέγγιση της 3GPP επιτρέπει την έκδοση πιστοποιητικών μόνο από το 3G HN. Επιπλέον, ο συγκεκριμένος μηχανισμός βασίζεται σε μια διαδικασία παραγωγής συμμετρικών κλειδιών, με την προϋπόθεση ότι ο χρήστης έχει αυθεντικοποιηθεί με επιτυχία σε κάποιο bootstrapping εξυπηρέτη, παρά σε ιδιωτικά κλειδιά. Επίσης, τα πιστοποιητικά που εκδίδονται μπορούν να χρησιμοποιηθούν μόνο για τη λήψη συγκεκριμένων υπηρεσιών που ελέγχονται από το 3G HN.

Η προτεινόμενη αρχιτεκτονική (Kambourakis et al., 2004g; Kambourakis et al., 2004h), η οποία εναρμονίζεται στο μέγιστο βαθμό με τις τεχνικές προδιαγραφές της 3GPP για ενοποιημένα WLAN-3G περιβάλλοντα (3GPP TS, 2004), αποτυπώνεται στο σχήμα 6-2. Οι διακρινόμενες CA/AA οντότητες είναι δυνατόν να εξασφαλίζονται από τους μηχανισμούς ασφάλειας του συγκεκριμένου τομέα. Αυτό σημαίνει ότι τα πρωτόκολλα και οι υπόλοιπες διαδικασίες που απαιτούνται για την εξασφάλιση των επικοινωνιών μεταξύ αυτών και των άλλων εμπλεκομένων οντοτήτων είναι ήδη διευθετημένα. Για παράδειγμα, όπως προσδιορίζεται στα (3GPP TS, 2004e; 3GPP TS, 2002), οι δια-δικτυακές και ενδο-δικτυακές επικοινωνίες μπο-

ρούν να προστατευτούν, χρησιμοποιώντας τα πρωτόκολλα MAPsec και IPsec (βλ. Κεφάλαιο 3).

Η συγκεκριμένη αρχιτεκτονική (βλ. σχήμα 6-2) εισάγει μια νέα δικτυακή οντότητα, η οποία λειτουργεί ως πύλη (gateway) παροχής υπηρεσιών ψηφιακών πιστοποιητικών (Certificate provisioning Gateway, CGW) για το χρήστη. Συνεπώς, νέες IP διεπαφές (interfaces) και πρωτόκολλα επικοινωνίας χρειάζεται να οριστούν μεταξύ των αντίστοιχων οντοτήτων, π.χ., μεταξύ της CGW και της αντίστοιχης CA/AA. Ασφαλώς, διάφορες άλλες εναλλακτικές λύσεις είναι επίσης δυνατές. Για παράδειγμα, η απευθείας σύνδεση της CA/AA με το GGSN (βλ. και ενότητα 2.3.2) φαίνεται να είναι μια «ελκυστική» και πάνω απ' όλα «φυσική» λύση, μιας και το GGSN αποτελεί τον κόμβο εξόδου και εισόδου από και προς άλλα δίκτυα. Παρόλα αυτά, μια τέτοια επιλογή θα ήταν δυνατό να υποστηρίξει την έκδοση πιστοποιητικών μόνο από 3GPP περιβάλλοντα. Επιπλέον, θα απαιτούσε τον καθορισμό νέων μηνυμάτων μεταξύ του UE και του SGSN, του GGSN και του SGSN, καθώς και στα ενεργά Packet Data Protocol (PDP) πλαίσια (contexts). Αν, για παράδειγμα, ο χρήστης επιθυμεί την έκδοση ενός πιστοποιητικού από κάποιο SN, το UE πρέπει να ενεργοποιήσει ένα δευτερεύον (secondary) PDP πλαίσιο, με την προϋπόθεση ότι κάτι τέτοιο επιτρέπεται από το SN.

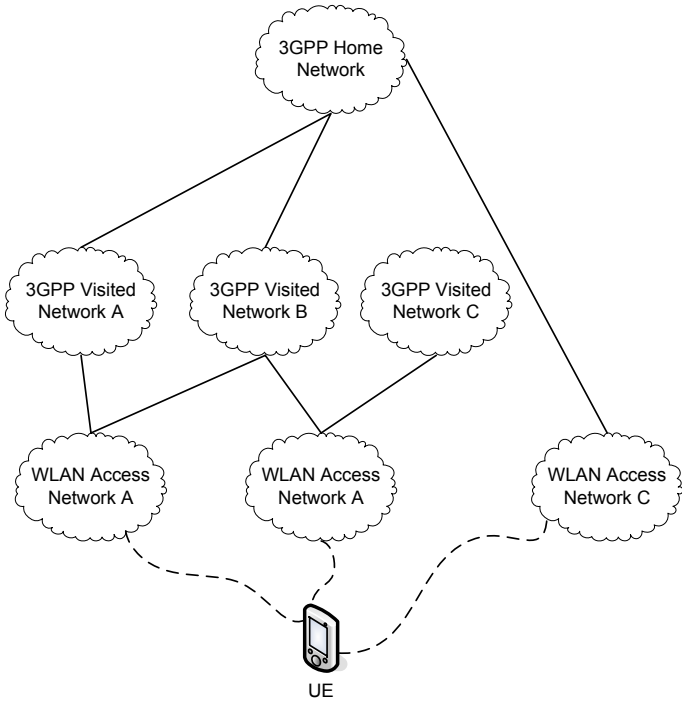


Σχήμα 6-2. Γενική αρχιτεκτονική για την υποστήριξη των υπηρεσιών αυθεντικοποίησης και έκδοσης ψηφιακών πιστοποιητικών σε ενοποιημένα περιβάλλοντα 3GPP-WLAN (συμβατό με το (3GPP TS, 2004))

Προφανώς, πριν να είναι σε θέση ο χρήστης να ζητήσει για παράδειγμα την έκδοση κάποιου πιστοποιητικού, θα πρέπει να αυθεντικοποιηθεί επιτυχώς από το δίκτυο. Για αυτό το σκοπό, η 3GPP φαίνεται να προτιμά πρωτόκολλο EAP-AKA, του οποίου η λειτουργία και τα ιδιαίτερα χαρακτηριστικά αναπτύχθηκαν στο Κεφάλαιο 5.

6.3. Περιγραφή και Απαιτήσεις

Στο σχήμα 6-3 παρουσιάζεται ένα σενάριο με βάση το οποίο ένας 3GPP χρήστης περιάγει σε περιοχή, που καλύπτεται από έναν αριθμό hot-spots. Εκτελώντας διαδικασίες ενεργητικής (active) ή παθητικής (passive) ανίχνευσης (IEEE Std, 1999), το τερματικό του χρήστη μπορεί να ανακαλύψει όλα τα διαθέσιμα αναγνωριστικά WLAN (Service Set Identifiers, SSID). Όταν η λίστα αυτή έχει ολοκληρωθεί, τότε το UE είναι σε θέση να συνδεθεί στο περισσότερο προτιμώμενο WLAN. Για παράδειγμα, το UE θα χρησιμοποιήσει το SSID, το οποίο διαθέτει απευθείας σύνδεση με το HN 3GPP δίκτυο. Αν αυτό δεν είναι εφικτό, τότε το UE μπορεί να επιλέξει ένα SSID, που διαθέτει σύνδεση με έναν από τους προτιμώμενους 3GPP παρόχους. Μια «λίστα 3GPP παρόχων ταξινομημένων κατά σειρά προτίμησης» είναι δυνατό να είναι αποθηκευμένη στη UICC.



Σχήμα 6-3. Σενάριο επιλογής δικτύου

Οι διαδικασίες επιλογής δικτύου και αυθεντικοποίησης βασίζονται στην αποστολή του NAI που ο χρήστης διαθέτει (βλ. ενότητα 5.2 και 3GPP TS, 2004b; Adrangi, 2004). Ο AAA εξυπηρέτης θα απαντήσει στο UE, υποδεικνύοντας το αποτέλεσμα της διαδικασίας αυθεντικοποίησης. Αν η τελευταία ήταν επιτυχής, ο AAA εξυπηρέτης θα επιστρέψει στο αντίστοιχο CGW επιπλέον πληροφορίες σχετικές με την έκδοση πιστοποιητικών (certificate-related) από

το profile του συνδρομητή, το οποίο βρίσκεται αποθηκευμένο στο HSS. Οι πληροφορίες αυτές θα επιτρέψουν στο CGW να αποφασίζει αν η έκδοση πιστοποιητικών για το συγκεκριμένο συνδρομητή είναι επιτρεπτή, ποια είδη πιστοποιητικών μπορούν να αποκτηθούν και από ποια δίκτυα, το αναγνωριστικό της συμφωνίας περιαγωγής που βρίσκει εφαρμογή σε κάθε περίπτωση κτλ.

Αφού λοιπόν ο χρήστης αυθεντικοποιηθεί και έχει αποκτήσει συγκεκριμένη IP διεύθυνση, το UE, ανάλογα με την περίπτωση, πρέπει να ανακαλύψει το κατάλληλο HN ή SN CGW. Στην πραγματικότητα, όπως αναφέρεται στο (3GPP TS, 2004), ο χρήστης μπορεί να αποκτήσει δύο IP διευθύνσεις: μια εσωτερική (inner) και μια εξωτερική (outer). Η διαδικασία αυτή είναι δυνατό να πραγματοποιηθεί με μια από τις παρακάτω τέσσερις μεθόδους:

- Οι διευθύνσεις των διαθέσιμων CGW θα δημοσιεύονται. Το UE θα αποθηκεύει όλες τις αναγκαίες παραμέτρους κατά τη διαδικασία εγκαθίδρυσης της IP σύνδεσης.
- Οι διευθύνσεις των διαθέσιμων CGW θα ωθούνται (pushed) αυτόματα από το δίκτυο στο UE.
- Τα διαθέσιμα CGW μπορεί να ανακαλύπτονται δυναμικά, με χρήση του πρωτοκόλλου (Dynamic Host Configuration Protocol (DHCP), μετά την απόδοση IP διεύθυνσης. Ο DHCP εξυπηρέτης θα πληροφορεί το UE με το όνομα τομέα (domain name) που βρίσκεται εγκατεστημένο το τοπικό CGW και τη διεύθυνση ενός εξυπηρέτη επίλυσης ονομάτων τομέων (Domain Name Server, DNS), ο οποίος είναι ικανός να επιλύσει το πλήρες όνομα (Fully Qualified Name, FQDN) του CGW.
- Κατά τη διάρκεια των διαδικασιών ενεργοποίησης ή ανανέωσης του πρωτεύοντος PDP πλαισίου (αν ο χρήστης διατηρεί μια απευθείας σύνδεση με το 3GPP HN).

Με βάση τα παραπάνω, η έκδοση ψηφιακών πιστοποιητικών για κάθε χρήστη είναι δυνατή οποιαδήποτε στιγμή, με την προϋπόθεση ότι κάτι τέτοιο δεν αντιτίθεται στα δικαιώματά του, όπως αυτά προσδιορίζονται στο profile του. Έτσι, ένα πιστοποιητικό μπορεί να ζητηθεί είτε από το CGW του HN, είτε από το αντίστοιχο του SN (αν υπάρχει). Το SN μπορεί να είναι ένα 3GPP ή ένα WLAN δίκτυο. Περισσότερες πληροφορίες και λεπτομέρειες σχετικά με τη διαδικασία έκδοσης πιστοποιητικών και τα προτεινόμενα πρωτόκολλα επικοινωνίας περιλαμβάνονται στην ενότητα 6.4.2.

Η διαδικασία απαιτεί από το UE να υποστηρίζει το μηχανισμό αυθεντικοποίησης EAP-AKA, ενώ παράλληλα τα profile των συνδρομητών θα πρέπει να ενημερωθούν ώστε να συμπεριλάβουν τα απαραίτητα πεδία σχετικά με την έκδοση ψηφιακών πιστοποιητικών. Αυτό θα επιτρέπει στον HN πάροχο να ελέγχει τις διαδικασίες έκδοσης πιστοποιητικών από τους συν-

δρομητές του. Για παράδειγμα, ποιοι τύποι πιστοποιητικών επιτρέπονται και σε ποιο συνδρομητή.

Όπως ήδη αναφέρθηκε παραπάνω, τα ζητήματα εμπιστοσύνης (trust issues) μεταξύ του HN και των SN παρόχων (3GPP TS, 2004c), ρυθμίζονται με βάση αντίστοιχες προκαθορισμένες συμφωνίες περιαγωγής ή παροχής υπηρεσιών (roaming or service agreements). Επιπλέον, οι υπηρεσίες PKI μπορούν να προσφέρονται από έναν 3GPP ή WLAN πάροχο, ή από ένα συνεργαζόμενο CSP. Σ' αυτή την περίπτωση, είναι απαραίτητο να λάβουμε υπόψη μας τις συμπληρωματικές συμφωνίες υπηρεσιών, οι οποίες πιθανόν να απαιτούνται μεταξύ των 3GPP/WLAN παρόχων και των αντίστοιχων CSPs.

Εκτός των άλλων, απαιτείται προτυποποίηση νέων μηνυμάτων με τη μορφή πρωτοκόλλων μεταξύ των CGW και του UE, και του CGW και του AAA εξυπηρέτη (για τη μεταφορά των απαραίτητων πεδίων που αφορούν πιστοποιητικά από το profile των συνδρομητών). Είναι επίσης φανερό ότι προκειμένου ο χρήστης να είναι ικανός να χρησιμοποιήσει τέτοιου είδους υπηρεσίες, πρέπει να διαθέτει μια διπλής λειτουργίας (dual mode) τερματική συσκευή, η οποία υποστηρίζει WLAN και 3G, ή η WLAN συσκευή του να μπορεί να συνδεθεί (μέσω Bluetooth, USB, IrDA) με άλλο εξοπλισμό, ο οποίος υποστηρίζει 3GPP υπηρεσίες. Το ιδιωτικό κλειδί του συνδρομητή μπορεί να αποθηκεύεται στη UICC κάρτα του, ενώ η προσπέλασή του από μια εφαρμογή θα είναι δυνατή, παρέχοντας ένα ξεχωριστό προσωπικό αριθμό PIN (ή συνθηματικό) γνωστό μόνο στο χρήστη (βλ. ενότητα 2.3.1, αρ. 3).

Συνοψίζοντας, η προτεινόμενη αρχιτεκτονική αποτελεί μια ανεξάρτητη του μέσου προσπέλασης (access independent) βασισμένη στο πρωτόκολλο IP προσέγγιση, η οποία είναι σχετικά εύκολο να υλοποιηθεί στους σύγχρονους 3GPP PS τομείς (PS domains), όπως το GPRS και σε υβριδικά 3GPP/WLAN περιβάλλοντα. Αυτό εξηγείται από το γεγονός ότι συνάγει στο μέγιστο βαθμό με τη 3GPP αρχιτεκτονική και παράλληλα απαιτεί ελάχιστες αλλαγές στα υπάρχοντα στοιχεία των κεντρικών δικτύων των παρόχων και στα πρωτόκολλα που αυτά χρησιμοποιούν. Επιπλέον, το συγκεκριμένο σχήμα δεν επηρεάζει τα τρέχοντα πρότυπα και τον ήδη εγκατεστημένο εξοπλισμό των WLAN δικτύων. Για παράδειγμα, δεν απαιτεί καμιά τροποποίηση στα APs, στην εκπομπή των SSIDs, κτλ.

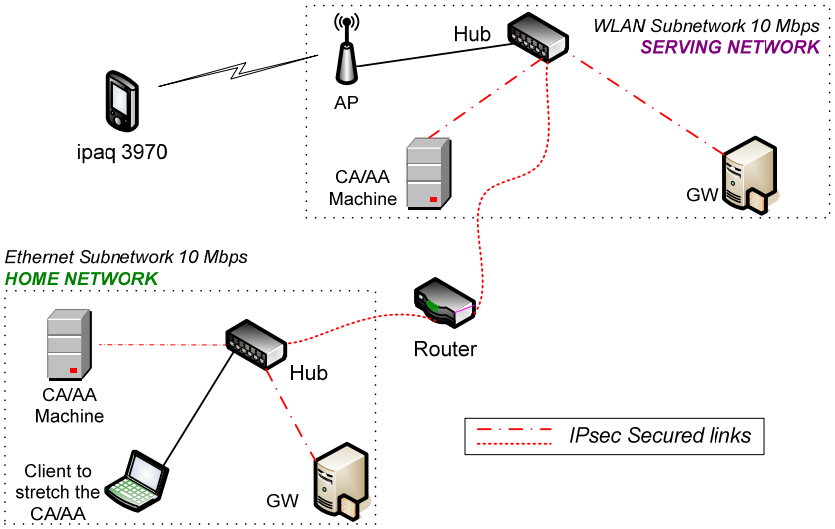
6.4. Πειραματική διάταξη για την έκδοση Πιστοποιητικών

6.4.1. Περιγραφή

Προκειμένου να εξετάσουμε την αποτελεσματικότητα της προτεινόμενης αρχιτεκτονικής (βλ. σχήμα 6-2), χρησιμοποιήσαμε ως μελέτη περίπτωσης την παράδοση AC πάνω από IEEE 802.11b και GPRS δίκτυα (Kambourakis et al., 2004g, Kambourakis et al., 2004). Δημιουργήσαμε δύο αρχιτεκτονικές δικτύου, οι οποίες παρουσιάζονται στα σχήματα 6-4 και 6-5. Η

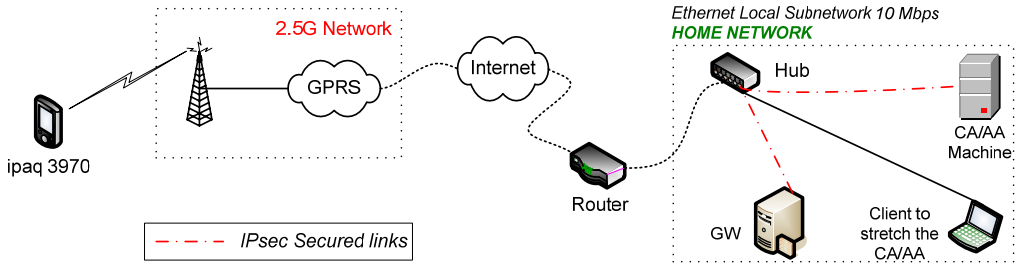
κύρια διαφορά μεταξύ αυτών των δύο τοπολογιών είναι ο τύπος του δικτύου στο οποίο συνδέεται ο χρήστης. Στο σχήμα 6-4, το SN είναι ένα WLAN, ενώ στο σχήμα 6-5, ο χρήστης συνδέεται στο HN μέσω GPRS. Η φορητή συσκευή που ο χρήστης διαθέτει είναι ένα iPAQ H3970 PCC, του οποίου τα χαρακτηριστικά περιγράφονται αναλυτικά στην ενότητα 4.4.1.

Οι δύο CGW μηχανές ενσωματώνουν επεξεργαστές P4 χρονισμένους στα 1GHz και 128 MB κύρια μνήμη και είναι εγκατεστημένες στα αντίστοιχα υπο-δίκτυα (HN & SN). Στην άλλη πλευρά, οι δύο CA/AA εξυπηρέτες διαθέτουν επεξεργαστές P4 χρονισμένους στα 1.4GHz και 192 MB κύρια μνήμη. Όλες οι παραπάνω μηχανές χρησιμοποιούν το λειτουργικό σύστημα Windows XP Professional της εταιρείας Microsoft. Το AP του σχήματος 6-4, είναι του τύπου DWL-900AP+ της εταιρείας D-Link και υποστηρίζει ταχύτητες από 10 έως 22 Mbps. Για τις ανάγκες του πειράματος η ταχύτητα του συγκεκριμένου AP ρυθμίστηκε στα 10 Mbps.



Σχήμα 6-4. Τοπολογία του σεναρίου Α

Όλες οι ενδο-δικτυακές επικοινωνίες μεταξύ των CA/AA και των CGWs και στα δύο σενάρια προστατεύονται από το πρωτόκολλο IPsec Authentication Header (AH) σε κατάσταση μεταφοράς (transport mode). Επίσης, οι δια-δικτυακές επικοινωνίες στην τοπολογία του σχήματος 6-4 προστατεύονται από το πρωτόκολλο IPsec Encapsulating Security Payload (ESP) σε κατάσταση διόδου (tunnel mode). Όπως είναι γνωστό, το πρωτόκολλο IPsec χρησιμοποιεί το πρωτόκολλο IKE για αυθεντικοποίηση των επικοινωνουσών οντοτήτων και την εγκαθίδρυση μιας SA. Το IKE μπορεί να ρυθμιστεί ώστε η αυθεντικοποίηση των μερών να χρησιμοποιεί προ-καθορισμένα (pre-shared) μυστικά κλειδιά ή PKCs (Public key-based authentication with certificates). Στα σενάριά μας, επιλέξαμε να χρησιμοποιήσουμε το πρωτόκολλο IKE σε κύρια κατάσταση, με ψηφιακές υπογραφές και PKCs (main mode with digital signatures and certificates). Σημειώνεται, ότι τα πρωτόκολλα IPsec και IKE με χρήση προ-καθορισμένων κλειδιών χρησιμοποιούνται και στο σύστημα UMTS για την εξασφάλιση των ενδο-δικτυακών και δι-δικτυακών επικοινωνιών των κεντρικών PS δικτύων των παρόχων (βλ. Κεφάλαιο 3).



Σχήμα 6-5. Τοπολογία του σεναρίου B

Οι εφαρμογές που χρησιμοποιήσαμε αναπτύχθηκαν με τη γλώσσα Embedded C++ της εταιρείας Microsoft στην έκδοση 4.0. Προκειμένου να ενσωματώσουμε τις απαραίτητες λειτουργίες δημόσιου κλειδιού στον κώδικα, χρησιμοποιήσαμε τη γνωστή κρυπτο-βιβλιοθήκη ή πακέτο ανοικτού κώδικα (open-source) OpenSSL στην έκδοση 0.9.7b (βλ. ενότητα 4.4.1). Η ίδια βιβλιοθήκη χρησιμοποιήθηκε για τη δημιουργία των απαραίτητων πιστοποιητικών. Ο απαιτούμενος χώρος στην κύρια μνήμη των μηχανών για την εκτέλεση των εφαρμογών του πελάτη, της CGW και της CA/AA, ήταν αντίστοιχα 100, 98 και 96.1 Kbytes.

Το GPRS Σχήμα κωδικοποίησης (coding scheme) ήταν το CS-1 (9.05 kb/s) και οι διαθέσιμες για το GPRS «θυρίδες χρόνου» (time slots) μεταβάλλονταν μεταξύ 3 και 4. Κατά συνέπεια η ταχύτητα του ασύρματου δικτύου κυμαινόταν από 27 έως 36 Kb/s. Οι διεργασίες των CA/AA εξυπηρετών και των CGW είναι πολυ-νηματικές (multi-threaded). Όταν λαμβάνουν μια αίτηση για έκδοση η προώθηση πιστοποιητικού, ενεργοποιούν ένα νήμα για να ανταποκριθούν και να την εξυπηρετήσουν. Επιπλέον, χρησιμοποιήσαμε μια ακόμα διεργασία, η οποία είχε ως σκοπό να «φορτώνει» τη CA/AA με ένα σημαντικό αριθμό αιτήσεων για έκδοση ACs. Η διεργασία αυτή εκτελείται σε μια διαφορετική φορητή (laptop) μηχανή, που ενσωματώνει επεξεργαστή Celeron χρονισμένο στα 1.2 GHz και 256 MB κύριας μνήμης και είναι εγκατεστημένη στο HN ή στο SN υπο-δίκτυο. Ο χρόνος μεταξύ δύο διαδοχικών αιτήσεων για έκδοση ACs ακολουθεί την αρνητικά εκθετική κατανομή (negative exponential distribution). Στην επόμενη ενότητα περιγράφουμε αναλυτικά τη διαδικασία απόκτησης ενός AC από την αντίστοιχη (ανάλογα με το σενάριο) CA/AA.

6.4.2. Αναλυτική περιγραφή της διαδικασίας απόκτησης ACs

Ο στόχος της παρούσας ενότητας είναι να περιγράψει τις λεπτομέρειες υλοποίησης σχετικά με τη δημιουργία και επεξεργασία αιτήσεων για έκδοση ACs. Ανάλογα με το είδος της αίτησης, ο χρήστης ή ένας αυτοματισμός (automaton – process, daemon, service), για λογαριασμό του χρήστη, δημιουργεί μια πιστοποιημένη αίτηση για έκδοση AC συμπληρώνοντας τιμές στα παρακάτω πεδία. Παρακάτω, παρέχουμε κάποιες ενδεικτικές τιμές (demo values). Όπως είναι φυσικό, ανάλογα με την υλοποίηση, η αίτηση μπορεί να περιλαμβάνει (ή να παραλείπει)

κάποια πεδία, όπως για παράδειγμα, το χρόνο δημιουργίας της αίτησης, τους προσδιοριστές των αλγορίθμων που χρησιμοποιήθηκαν για σύνοψη και υπογραφή, κτλ.

COUNTRYNAME = "US"

STATEORPROVINCENAME = "VA"

LOCALITYNAME = "FAIRFAX"

ORGANIZATIONNAME = "ZORG.ORG"

ORGANIZATIONALUNITNAME = "SERVER DIVISION"

COMMONNAME = "NAI(IMSI/P-TMSI@realm)"

SUBJECTALTNAME = "DNS:195.251.161.167"

TYPEOFREQUEST = "0.000" (bit pattern)

Το έκτο πεδίο προσδιορίζει το P-TMSI (3GPP TS, 2004c), το οποίο ανατίθεται στο UE από τον AAA εξυπηρέτη, κατά τη διάρκεια της διαδικασίας αυθεντικοποίησης. Αν το P-TMSI δεν είναι διαθέσιμο, τότε υπάρχει η δυνατότητα να χρησιμοποιηθεί το IMSI. Το τελευταίο πεδίο δηλώνει τον τύπο του AC που ο χρήστης επιθυμεί (τα τρία τελευταία ψηφία) και το δίκτυο από το οποίο αυτό θα εκδοθεί (το πρώτο ψηφίο). Για παράδειγμα, η τιμή «1.101» υποδηλώνει «SN» και «Τύπος αίτησης = 101».

Όταν η φάση συμπλήρωσης των πεδίων της αίτησης έχει ολοκληρωθεί, η σχετική εφαρμογή προσθέτει σ' αυτή το δημόσιο κλειδί του συνδρομητή και δημιουργεί μια σύνοψη χρησιμοποιώντας τη συνάρτηση MD5. Επίσης, η σύνοψη κρυπτογραφείται (ενθυλακώνεται) με το RSA 1024 bits ιδιωτικό κλειδί του συνδρομητή και προστίθεται στην αίτηση. Αναλυτικότερα, 16_bytes Σύνοψη = MD5(Αίτηση + Δημ_Κλειδί_Χρήστη) και Ψηφιακή_Υπογραφή = (Σύνοψη) $_{\text{Ιδιωτικό\_Κλειδί\_Χρήστη}}$.

Η αυθεντικοποιημένη με τον παραπάνω τρόπο, μεγέθους περίπου 740 bytes, αίτηση (Αίτηση || Δημόσιο κλειδί του χρήστη || Ψηφιακή Υπογραφή), μεταδίδεται κατόπιν στο CGW του SN δικτύου. Μόλις το τελευταίο λάβει την αίτηση, επαληθεύει την υπογραφή της (δημιουργεί εκ νέου τη σύνοψη, αποκρυπτογραφεί την υπογραφή, χρησιμοποιώντας το δημόσιο κλειδί του συνδρομητή, συγκρίνει τις δύο συνόψεις). Έτσι, πιστοποιεί ότι η αίτηση δεν έχει υποστεί κάποια ανεπιθύμητη αλλαγή. Όταν η διαδικασία επαλήθευσης ολοκληρωθεί με επιτυχία, το CGW ελέγχει το πρώτο ψηφίο του τελευταίου πεδίου ώστε να αποφασίσει πού πρέπει να τη δρομολογήσει. Ο παραλήπτης μπορεί να είναι η τοπική CA/AA ή κάποιο άλλο CGW στο HN δίκτυο. Εννοείται ότι στην περίπτωση που το SN ταυτίζεται με το HN δίκτυο του χρήστη, η αίτηση μπορεί να σταλεί μόνο στην τοπική (HN) CA/AA. Πριν τη μετάδοση, το CGW είναι δυνατό να επισυνάψει στην αίτηση και άλλες παραμέτρους (σχετικές με την έκδοση πιστοποιητικών) από το profile του χρήστη (βλ. ενότητα 6.3). Αυτές απαιτούνται από τη CA/AA προκειμένου να εκδώσει το AC. Εναλλακτικά, η επαλήθευση της αίτησης είναι εφικτό να

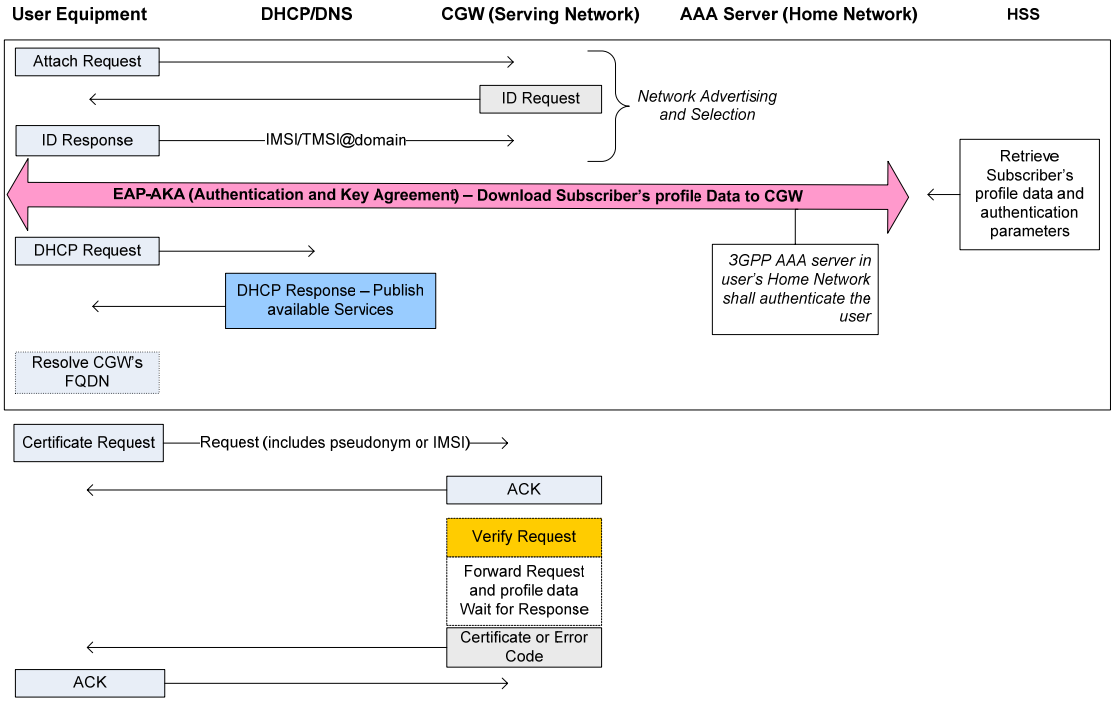
εκτελεστεί στο τελικό CGW, αντί στο CGW του SN. Παρόλα αυτά, αν η αίτηση δεν είναι έγκυρη εξ αρχής, τότε θα προωθηθεί χωρίς λόγο στο τελικό CGW, το οποίο θα την απορρίψει, δημιουργώντας τον κατάλληλο κωδικό λάθους (βλ. σχήμα 6-7).

Με την παραλαβή της αίτησης, η CA/AA θα εκδώσει και θα υπογράψει με το ιδιωτικό κλειδί της το κατάλληλο AC. Τα εκδιδόμενα ACs μπορούν να αποθηκεύονται σε κάποια αποθήκη πιστοποιητικών (certificate repository), η οποία είναι δυνατό να έχει, για παράδειγμα, τη μορφή ενός Lightweight Directory Access Protocol (LDAP) εξυπηρέτη (Wahl et al., 1997). Ακολούθως, η CA/AA θα αποστείλει το AC πίσω στο χρήστη, ακολουθώντας μια από τις παρακάτω διαδρομές:

(α) CA/AA (HN ή SN) → CGW (HN ή SN) → UE.

(b) CA/AA (HN) → CGW (HN) → CGW (SN) → UE.

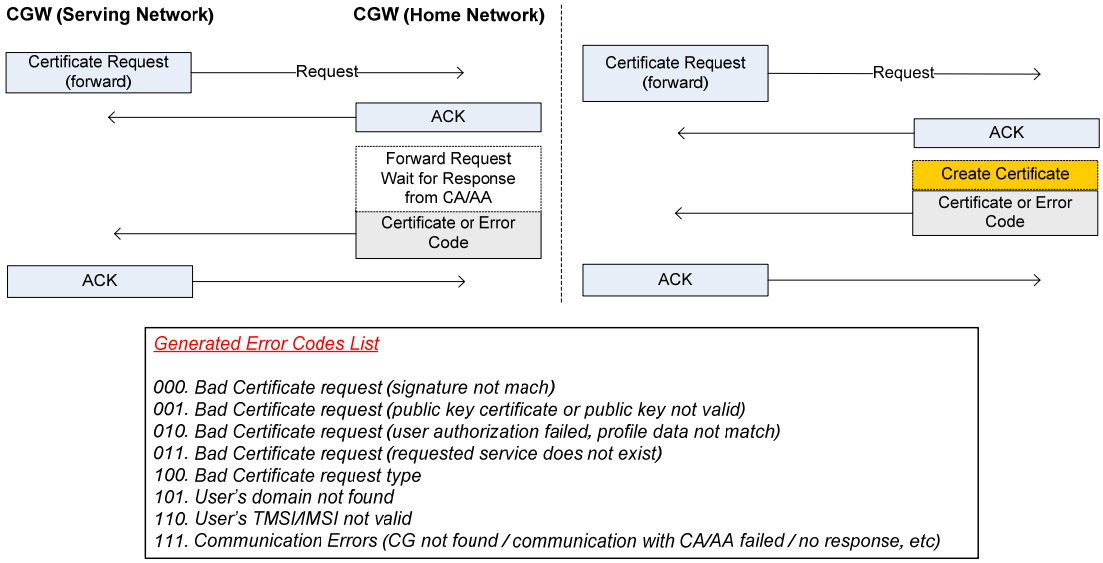
Όλες οι παραπάνω ανταλλαγές μηνυμάτων μεταξύ των επικοινωνουσών οντοτήτων έχουν οργανωθεί σε απλά πρωτόκολλα επικοινωνίας, τα οποία παρουσιάζονται στα σχήματα 6-6 και 6-7.



Σχήμα 6-6. Πρωτόκολλο επικοινωνίας μεταξύ UE και CGW στο SN

Όταν το AC παραδοθεί στο χρήστη, αυτός είναι δυνατό να το χρησιμοποιήσει σύμφωνα με το μοντέλο *push* (Farrell & Housley, 2002). Εναλλακτικά, το UE έχει τη δυνατότητα να μεταβιβάσει (pass) στον εξυπηρέτη εφαρμογών (application server), αντί του πραγματικού AC, το σύνδεσμο στον οποίο το AC βρίσκεται αποθηκευμένο (μοντέλο *pull*). Επίσης, τα σχετικά με την έκδοση ACs ιστορικά στοιχεία (records), τα οποία διατηρούνται στην CA/AA, μπορούν

να παρέχουν υπηρεσίες μη-αποποίησης. Για παράδειγμα, έστω ότι κάποιος διατηρεί ένα λογαριασμό σε ένα μεσιτικό γραφείο άμεσης πρόσβασης (on-line brokerage) και αγοράζει μετοχές, χρησιμοποιώντας σχετική εφαρμογή που εκτελείται στη φορητή συσκευή του. Αμέσως μετά, σκοπίμως, αρνείται τη συγκεκριμένη συναλλαγή. Στην πραγματικότητα είναι πολύ δύσκολο για το μεσίτη να αποδείξει ότι ο πελάτης του πράγματι αγόρασε τις εν λόγω μετοχές. Παρόλα αυτά, αν η εφαρμογή είχε χρησιμοποιήσει για την πράξη αγοράς κάποιο AC, ο μεσίτης θα μπορούσε εύκολα να αποδείξει ότι η συναλλαγή έλαβε χώρα.



Σχήμα 6-7. Πρωτόκολλα επικοινωνίας CGW-με-CGW, CGW-με-CA/AA και παραγόμενοι κωδικοί λαθών

6.4.3. Αναγνώριση πιθανών επιθέσεων

Η ενότητα αυτή προσπαθεί να προσδιορίσει την ταυτότητα επιθέσεων που είναι δυνατό να εκδηλωθούν κατά τη διάρκεια των διαδικασιών αίτησης έκδοσης και παράδοσης ACs. Οι πιθανές απειλές προσδιορίζονται είτε στην εμπιστευτικότητα και ακεραιότητα των διακινούμενων δεδομένων (αιτήσεις, ACs, δεδομένα των profiles των συνδρομητών), είτε στην ακεραιότητα των μηνυμάτων σηματοδοσίας (signaling), μεταξύ των επικοινωνουσών οντοτήτων. Επίσης, διάφορες άλλες, σχετικές με τα προηγούμενα επιθέσεις είναι δυνατό να πραγματοποιηθούν, όπως επιθέσεις τύπου παρακώλυσης της διαθεσιμότητας των υπηρεσιών (Denial of Service, DoS) και μη-εξουσιοδοτημένης χρήσης του ιδιωτικού κλειδιού του χρήστη. Άλλα είδη απειλών, όπως οι ραδιο-παρεμβολές (radio jamming) δεν εξετάζονται.

Στις περισσότερες περιπτώσεις, μετά το τέλος της διαδικασίας αυθεντικοποίησης, η κρυπτογράφηση των δεδομένων και η προστασία της ακεραιότητας των μηνυμάτων σηματοδοσίας μεταξύ του UE και του AP (ή του RNC) έχει ενεργοποιηθεί. Παρόλα αυτά, αν, για παράδειγμα, υποθέσουμε ότι η διαδικασία κρυπτογράφησης βασίζεται σε αδύνατους αλγόριθμους, μία

επίθεση είναι εφικτό να πραγματοποιηθεί μόνο στην ασύρματη ζεύξη (link), μιας και η ακεραιότητα και η εμπιστευτικότητα των δεδομένων στα ενσύρματα τμήματα των δικτύων προστατεύεται από το πρωτόκολλο IPsec (βλ. ενότητα 6.4.1). Για παράδειγμα, μια επίθεση του τύπου MITM (ή απλώς η παρακολούθηση της κίνησης (traffic) γύρω από ένα AP), μπορεί να επιτρέψει στον εισβολέα να υποκλέψει αιτήσεις ή ακόμα και ACs. Παρόμοιοι κίνδυνοι διακρίνονται σε επιθέσεις του τύπου πλαστών (rogue) APs, όπου ο επιτιθέμενος «μεταμφιέζει» (masquerade) ένα δικό του AP σε «νόμιμο» (legitimate) με στόχο να υποκλέψει πληροφορίες.

Όμως, ακόμη και στην περίπτωση που αυτός τα καταφέρει, δε θα είναι σε θέση να χαλκεύσει (forge) την αίτηση ή το AP και έτσι να το χρησιμοποιήσει για δικό του λογαριασμό, αφού δεν διαθέτει το ιδιωτικό κλειδί του χρήστη ή της CA/AA το οποίο απαιτείται ώστε να αναπαράγει τη σωστή υπογραφή. Με βάση τα παραπάνω, οι αιτήσεις και τα ACs μπορούν να αποστέλλονται ακόμη και σε μορφή καθαρού κειμένου (clear-text), με δεδομένο ότι δεν εξυπηρετούν τους περισσότερους από τους στόχους του πιθανού εισβολέα. Σε ορισμένες όμως περιπτώσεις, όπως για παράδειγμα σ' αυτές που το AC περιέχει ευαίσθητα δεδομένα (π.χ. το πεδίο του κατόχου), υπάρχει η δυνατότητα το AC να κρυπτογραφείται από την CA/AA, με το δημόσιο κλειδί του χρήστη, πριν αποσταλεί πίσω στο UE. Το γεγονός αυτό εξυπηρετεί δύο επιπλέον στόχους. Επιτρέπει στο UE να επαληθεύσει την ακεραιότητα του ληφθέντος AC, αποκρυπτογραφώντας το με το ιδιωτικό κλειδί του συνδρομητή και επιπλέον διασφαλίζει την CA/AA ότι το AC μπορεί να χρησιμοποιηθεί μόνο από τον εξουσιοδοτημένο χρήστη.

Εναλλακτικά, αντί του AC, είναι δυνατό να επιστραφεί στο UE ένας σύνδεσμος ή δείκτης (pointer), ο οποίος θα περιέχει τις απαραίτητες πληροφορίες (π.χ. σύνδεσμο (URL), όνομα σύνδεσης (login name), συνθηματικό), ώστε ο χρήστης να μπορέσει να ανακτήσει το AC. Σε κάθε περίπτωση, όμως, η ανάκτηση και προώθηση του πιστοποιητικού στον εξυπηρέτη εφαρμογών είναι προτιμότερο να γίνει από το χρήστη. Αν ο τελευταίος παραδώσει στον εξυπηρέτη εφαρμογών ένα URL αντί του πραγματικού AC, τότε θα πρέπει ο εξυπηρέτης να ανακτήσει το πιστοποιητικό. Σ' αυτή την περίπτωση, ο κίνδυνος μιας DoS επίθεσης είναι ορατός. Για παράδειγμα, όταν ο πελάτης σκοπίμως παραδίδει λανθασμένες URL στον εξυπηρέτη.

Διάφορες άλλες επιθέσεις του τύπου DoS είναι επίσης πιθανές. Για παράδειγμα, με τροποποίηση των αιτήσεων ή των ACs. Μια άλλου τύπου απειλή είναι γνωστή ως κατανεμημένη επίθεση DoS (Distributed DoS, DDoS). Οι επιθέσεις αυτού του τύπου με χρήση *"bots"* προέρχονται συνήθως από το Διαδίκτυο και μπορούν να στοχεύουν στη διαθεσιμότητα των CGW ή των AAA εξυπηρετών. Τα bots (robots), μπορούν για παράδειγμα να «αφουγκράζονται» (listen) για συνδέσεις στις θύρες (ports) των CGWs, περιμένοντας για μια συγκεκριμένη εντολή από τον επιτιθέμενο. Όταν αυτό συμβεί, αρχίζουν να πλημμυρίζουν (flooding) μια συγκεκριμένη IP διεύθυνση με πακέτα (packets).

Μια άλλη απειλή είναι γνωστή με το όνομα «υποκλοπή υπηρεσιών» (*service spoofing*). Σύμφωνα μ' αυτή, ο επιτιθέμενος υποδύεται μια ή περισσότερες υπηρεσίες στο τοπικό δίκτυο (π.χ. έναν DNS ή DHCP εξυπηρέτη ή μια CGW). Μια επίθεση αυτού του τύπου είναι δυνατό να εκδηλωθεί, χρησιμοποιώντας ένα «ψεύτικο» (rogue) AP. Παρόμοια με την προηγούμενη απειλή, είναι η επίθεση τύπου MITM, όπου ο επιτιθέμενος μπορεί να αντιστοιχίσει τις διευθύνσεις MAC ή/και IP της WLAN συσκευής του με την ταυτότητα ενός εξουσιοδοτημένου χρήστη. Έτσι, ο επιτιθέμενος έχει τη δυνατότητα να προσπελάσει πόρους και υπηρεσίες, οι οποίες είναι κανονικά προσβάσιμες (accessible) μόνο από τον εξουσιοδοτημένο χρήστη.

Τα σύγχρονα τερματικά ανοικτής πλατφόρμας (open platform terminals) μπορούν να προσβληθούν από ιούς (viruses), δούρειους ίππους (Trojan) ή άλλου είδους κακόβουλο λογισμικό. Έτσι, αν το περιβάλλον εκτέλεσης του ME δεν είναι ασφαλές, ο επιτιθέμενος είναι σε θέση να εγκαταστήσει ένα πρόγραμμα, το οποίο δείχνει στο χρήστη την απόκτηση ενός AC για «την αγορά μετοχών αξίας 10 €», αλλά ζητάει από τη USIM να υπογράψει μια διαφορετική αίτηση π.χ. για «την αγορά μετοχών αξίας 1000 €». Ακόμη χειρότερα, σε περίπτωση που το συγκεκριμένο πρόγραμμα καταφέρει να αποκτήσει πρόσβαση στο ιδιωτικό κλειδί του χρήστη, μπορεί να δημιουργήσει αυθαίρετο αριθμό υπογραφών, πριν ο χρήστης το αντιληφθεί. Έτσι, ο συνδρομητής θα πρέπει να πληρώσει για υπηρεσίες τις οποίες στην πραγματικότητα δεν έλαβε. Οι δούρειοι ίπποι μπορούν να εκτελέσουν παρόμοιες ενέργειες, όπως για παράδειγμα, να παρακολουθούν το πληκτρολόγιο του UE για συνθηματικά και PINs και κατόπιν να τα προωθούν στη μηχανή του επιτιθέμενου. Σε κάθε περίπτωση, το ιδιωτικό κλειδί του συνδρομητή είναι περισσότερο προστατευμένο, όταν αποθηκεύεται στη UICC παρά στο ME.

Αν το ψευδώνυμο του συνδρομητή (P_TMSI) δεν είναι διαθέσιμο, τότε στην αίτηση για την απόκτηση κάποιου AC, πρέπει να συμπεριληφθεί το IMSI. Το γεγονός αυτό αποτελεί απειλή για την ιδιωτικότητα (privacy) του συνδρομητή, μιας και ο επιτιθέμενος είναι σε θέση να εντοπίσει ποιος λαμβάνει το AC και πού αυτός κινείται (location privacy). Επίσης, όπως ήδη αναφέρθηκε στην ενότητα 6.1, τα ACs έχουν περιορισμένη χρονική ισχύ, πράγμα που σημαίνει ότι δεν απαιτείται η υλοποίηση διαδικασιών ανάκλησης. Ο κάτοχος ενός AC είναι υποχρεωμένος να το χρησιμοποιήσει πριν τη λήξη του.

6.5. Αποτελέσματα Μετρήσεων

6.5.1. Περιγραφή των χρόνων εξυπηρέτησης

Κατά τη διάρκεια των υπολογισμών μας χρησιμοποιήσαμε διάφορες τιμές για την παράμετρο λ, η οποία εκφράζει τον εικονικό επεξεργαστικό φόρτο που προσφέρεται στη CA/AA μέσω του ρυθμού αφίξεων των αιτήσεων για έκδοση ACs. Παρόλο ότι μεταβάλλαμε τις τιμές της συγκεκριμένης παραμέτρου από 20 έως 60 αιτήσεις το λεπτό, η επίδραση στην απόδοση του

εξυπηρέτη ήταν αμελητέα. Οι μετρήσεις συλλέχθηκαν από ένα σύνολο 2000 συναλλαγών μεταξύ του πελάτη (UE) και της CA/AA, οι οποίες πραγματοποιήθηκαν σε διαφορετικές ημέρες και ώρες σε περίοδο μιας εβδομάδας. Επίσης, το 50% των μετρήσεων πραγματοποιήθηκαν σε ώρες αιχμής (peak hours). Παρακολουθήσαμε και καταγράψαμε τους ακόλουθους χρόνους (πίνακας 6-1):

Χρόνος	**Περιγραφή**	**Σημασία**
Πελάτης		
CRCT	Client Request Creation Time	Ο χρόνος για το UE να δημιουργήσει την αίτηση. Η διαδικασία εκτελείται από ένα αυτοματισμό ή δαίμονα (daemon), ο οποίος είναι εγκατεστημένος στο UE.
CRTT	Client Request Transmission Time	Ο χρόνος που μεσολαβεί από την εκπομπή της αίτησης μέχρι το UE να λάβει από το CGW του SN/HN μήνυμα ACK (η αίτηση παραδόθηκε επιτυχώς στο CGW).
CRRT	Client Request Return Time	Ο χρόνος που μεσολαβεί από το CGW-ACK μέχρι την παραλαβή του AC από το UE.
CROT	Client Request Overall Time	Ο χρόνος που μεσολαβεί από την εκπομπή της αίτησης μέχρι την παραλαβή του AC από το UE και την αποστολή ενός μηνύματος ACK πίσω στο CGW. Ο χρόνος αυτός περιλαμβάνει τους CRTT και CRRT.
CGW		
CWVT	CGW request Verify Time	Ο χρόνος για το CGW να ελέγξει την εγκυρότητα της αίτησης (υπολογισμός σύνοψης, έλεγχος υπογραφής, λήψη απόφασης για το πού η αίτηση θα δρομολογηθεί).
CWFT	CGW request Forward Time	Ο χρόνος που μεσολαβεί από την προώθηση της αίτησης μέχρι τη λήψη μηνύματος ACK από τη CA/AA (Η αίτηση έχει παραληφθεί με επιτυχία).
CWOT	CGW Overall Time	Ο χρόνος που μεσολαβεί από την προώθηση της αίτησης μέχρι το AC να είναι διαθέσιμο στο CWG.
CA/AA		
AACT	AA certificate Creation Time	Χρόνος για την CA/AA να δημιουργήσει το AC ανάλογα με την ληφθείσα αίτηση.
AART	AA certificate Return Time	Ο χρόνος που μεσολαβεί από την προώθηση του AC, μέχρι η CA/AA να λάβει ένα μήνυμα ACK από το CGW (Το AC έχει παραληφθεί επιτυχώς από το CGW).

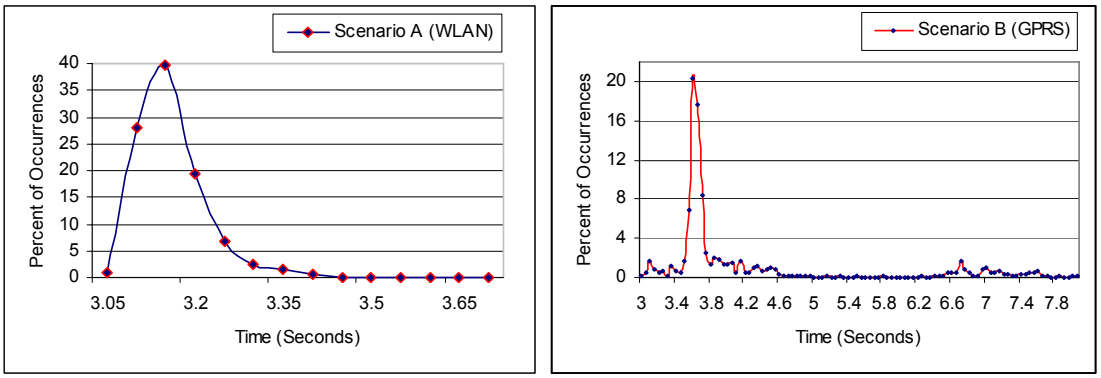
Πίνακας 6-1. Περιγραφή των χρόνων εξυπηρέτησης

6.5.2. Σενάριο A: Το SN δίκτυο είναι WLAN

Η τοπολογία του σεναρίου Α παρουσιάζεται στο σχήμα 6-4. Αποτελείται από δύο υπο-δίκτυα με μέσο χρόνο ping μεταξύ αυτών περίπου 80 milliseconds. Οι αιτήσεις παραδίδονται στο CGW του SN (WLAN) δικτύου και κατόπιν προωθούνται στο CGW του HN. Όλα τα ACs εκδίδονται από τη CA/AA του HN δικτύου. Οι μέσοι όροι και οι διακυμάνσεις των χρόνων εξυπηρέτησης (βλ. πίνακα 6-1), παρουσιάζονται στον πίνακα 6-2. Επίσης, το PDF διάγραμμα του χρόνου CROT παρουσιάζεται στην αριστερή πλευρά του σχήματος 6-8.

Χρόνος	*CRCT*	*CRTT*	*CRRT*	*CROT*	*GWVT*	*GWFT*	*GWOT*	*AACT*	*AART*
M.O.	1074.3	2955.8	144.1	3144.9	10.8	0.6	73.8	62.1	0.2
S.D.	31.1	92.6	171.8	196.6	55.0	5.7	26.2	11.3	1.0

Πίνακας 6-2. Μέσοι όροι και διακύμανση των χρόνων εξυπηρέτησης για το σενάριο Α



Σχήμα 6-8. PDF διαγράμματα για το χρόνο CROT (Σενάρια Α & Β)

6.5.3. Σενάριο B: Το SN δίκτυο είναι GPRS

Η τοπολογία του σεναρίου Β παρουσιάζεται στο σχήμα 6-5. Αποτελείται από δύο υπο-δίκτυα με μέσο χρόνο ping μεταξύ αυτών περίπου 1230 milliseconds. Ο πελάτης συνδέεται στο HN δίκτυο μέσω GPRS και κατά συνέπεια οι αιτήσεις για έκδοση πιστοποιητικών παραδίδονται στο τοπικό CGW (HN). Όλα τα ACs εκδίδονται από τη CA/AA του HN δικτύου. Οι μέσοι όροι και οι διακυμάνσεις των χρόνων εξυπηρέτησης (βλ. πίνακα 6-1), παρουσιάζονται στον πίνακα 6-3. Επίσης, το PDF διάγραμμα του χρόνου CROT παρουσιάζεται στη δεξιά πλευρά του σχήματος 6-8.

Χρόνος	*CRCT*	*CRTT*	*CRRT*	*CROT*	*GWVT*	*GWFT*	*GWOT*	*AACT*	*AART*
M.O.	1087.1	1543.4	2212.0	4361.4	7.5	3.9	70.2	59.7	0.3
S.D.	32.4	1095.2	1499.2	1797.8	5.7	4.9	25.3	8.0	1.1

Πίνακας 6-3. Μέσοι όροι και διακύμανση των χρόνων εξυπηρέτησης για το σενάριο Β

6.5.4. Παρατηρήσεις επί των αποτελεσμάτων

Όπως παρατηρούμε, ο μέσος χρόνος που απαιτείται για την ολοκλήρωση μιας συναλλαγής, (απόκτηση ενός AC) είναι περίπου 3.2 sec, όταν ο χρήστης συνδέεται σε ένα WLAN δίκτυο, και 4.4 sec, όταν συνδέεται μέσω GPRS. Η ίδια εικόνα αποτυπώνεται στα αντίστοιχα PDF διαγράμματα του σχήματος 6-8. Θα ήταν ίσως περισσότερο λογικό, οι συγκεκριμένοι χρόνοι να διαφέρουν αρκετά περισσότερο μεταξύ τους. Παρόλα αυτά, θα πρέπει να λάβουμε υπόψη μας τον επιπλέον χρόνο που απαιτείται στο σενάριο Α για την επικοινωνία CGW-με-CGW (round-trip).

Οι μέσοι όροι των χρόνων του GPRS και WLAN σεναρίων είναι συγκεντρωμένοι γύρω από την τιμή των 3.8 και 3.2 δευτερολέπτων αντίστοιχα. Οι χρόνοι αυτοί αναμένεται να αυξάνονται ανάλογα με την απόσταση (ping) μεταξύ των SN και HN δικτύων. Όσο μεγαλύτερος είναι ο αριθμός των δικτυακών τομέων που η αίτηση πρέπει να διασχίσει, τόσο μεγαλύτερος αναμένεται να είναι και ο μέσος χρόνος CROT. Οι αυξημένοι χρόνοι διακύμανσης που παρατηρούνται στο σενάριο Β, εξηγούνται από την αναξιοπιστία (unreliability) που γενικά χαρακτηρίζει μια GPRS σύνδεση. Από την άλλη πλευρά, οι αντίστοιχοι χρόνοι για το σενάριο Α χαρακτηρίζονται ως φυσιολογικοί.

Μία άλλη σημαντική παρατήρηση για το σενάριο Β είναι η επιπλέον καθυστέρηση που προκύπτει από το γεγονός ότι το CGW και η CA/AA δεν είναι εγκατεστημένα μέσα στο κεντρικό δίκτυο του 3G παρόχου. Κατά συνέπεια, η αίτηση και το AC θα πρέπει να διασχίσουν όλη τη διαδρομή πίσω, μέχρι το τοπικό δίκτυο, όπου το CGW και η CA/AA είναι εγκατεστημένα. Λαμβάνοντας υπόψη το μέσο χρόνο ping μεταξύ αυτών των δικτυακών τομέων, μπορούμε να εκτιμήσουμε το πόσο σημαντική είναι η καθυστέρηση αυτή. Φυσικά, ο συγκεκριμένος χρόνος αναμένεται να διαφέρει ανάλογα με την απόσταση μεταξύ των SGSN, CGW και της CA/AA στο κεντρικό δίκτυο του παρόχου.

6.6. Σύνοψη – Συμπεράσματα

Με τη διείσδυση της IP τεχνολογίας στα δίκτυα κινητών επικοινωνιών, οι πάροχοι και οι χρήστες των υπηρεσιών άρχισαν να αντιλαμβάνονται την ανάγκη για ισχυρούς μηχανισμούς προστασίας. Έτσι, ο ολοένα και περισσότερο αυξανόμενος αριθμός των χρηστών απαιτεί από τους παρόχους να προσφέρουν αξιόπιστους μηχανισμούς αυθεντικοποίησης, εξουσιοδότησης και καταγραφής, καθώς και υψηλή διαθεσιμότητα και ποιότητα υπηρεσιών ανάλογη με αυτή των ενσύρματων δικτύων.

Βασιζόμενοι στην υπόθεση ότι η απαραίτητη τεχνολογία PKI βρίσκεται προ των θυρών των κινητών δικτύων επικοινωνιών, προτείναμε και αναλύσαμε μία πρακτικά υλοποιήσιμη 3G-WLAN υβριδική αρχιτεκτονική, η οποία είναι πλήρως συμβατή με τις τελευταίες τεχνικές

προδιαγραφές της 3GPP, ενώ ταυτόχρονα είναι ικανή να παρέχει ψηφιακά πιστοποιητικά στους συνδρομητές. Η βασική ιδέα στηρίζεται σε μια νέα δικτυακή οντότητα, η οποία εισάγεται στο κεντρικό δίκτυο του 3GPP ή/και WLAN παρόχου και λειτουργεί ως πύλη (gateway) παροχής υπηρεσιών ψηφιακών πιστοποιητικών για τους χρήστες.

Η ανάλυσή μας εστιάστηκε στην παροχή πιστοποιητικών ιδιοτήτων, μιας και αυτά μπορούν να συνεισφέρουν σε υπηρεσίες εξουσιοδότησης των συνδρομητών, ενώ ταυτόχρονα, λόγω της προσωρινής φύσης τους, δεν απαιτούν την υλοποίηση διαδικασιών ανάκλησης. Παρόλα αυτά, υπάρχει η δυνατότητα το προτεινόμενο μοντέλο να χρησιμοποιηθεί ως βάση για προσφορά υπηρεσιών έκδοσης και διαχείρισης οποιονδήποτε τύπων ψηφιακών πιστοποιητικών. Επιπλέον, αναλύσαμε πιθανές απειλές που προκύπτουν από την υλοποίηση της συγκεκριμένης αρχιτεκτονικής, προτείνοντας, όπου αυτό ήταν δυνατό, τρόπους αντιμετώπισής τους.

Προκειμένου, να δοκιμάσουμε την αποτελεσματικότητα του προτεινόμενου σχήματος, χρησιμοποιήσαμε δύο πρότυπες αρχιτεκτονικές. Οι χρόνοι εξυπηρέτησης τόσο σε δίκτυα με τεχνολογία πρόσβασης 802.11, όσο και σε GPRS, αποδεικνύουν ότι η έκδοση πιστοποιητικών για τους συνδρομητές είναι κατορθωτή, ενώ ταυτόχρονα μπορεί να προσφέρει ευέλικτες και κλιμακούμενες λύσεις στους 3GPP παρόχους.

Μέρος Γ': Επίλογος

Κεφάλαιο 7: Συμπεράσματα και προοπτικές περαιτέρω έρευνας

Βιβλιογραφικές αναφορές

Κεφάλαιο 7: Συμπεράσματα και προοπτικές περαιτέρω έρευνας

7.1. Σύνοψη και συμπεράσματα

Η εξέλιξη των συστημάτων κινητών επικοινωνιών, έχοντας διανύσει ήδη απόσταση δυόμισι γενιών, βρίσκεται πλέον στις απαρχές της τρίτης. Η διείσδυση των υπηρεσιών κινητής τηλεφωνίας, των σύντομων μηνυμάτων κειμένου (Short Message Service, SMS) και τελευταία του GPRS και των πολυμεσικών μηνυμάτων (WAP, Multimedia Messaging Service, MMS, i-mode) στο πλατύ κοινό υπήρξε εντυπωσιακή. Παράλληλα, τα ζητήματα που αφορούν την ασφάλεια των κινητών δικτύων επικοινωνιών άρχισαν, ήδη από την πρώτη γενιά, να συγκεντρώνουν το ενδιαφέρον τόσο των επαγγελματιών και επιστημόνων της πληροφορικής, όσο και του κοινού ευρύτερα. Σήμερα, το ενδιαφέρον αυτό κορυφώνεται, ενώ ταυτόχρονα αποτελεί ζήτημα μεγάλης σημασίας για το σχεδιασμό των επερχόμενων συστημάτων κινητών επικοινωνιών $4^{ης}$ γενιάς (βλ. Κεφάλαιο 1).

Η τεχνολογία υποδομής δημόσιου κλειδιού αποτελεί μια από τις πλέον ενδιαφέρουσες τάσεις της ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων. Τα βασικά της πλεονεκτήματα είναι η εύκολη κλιμάκωση των μηχανισμών της σε οποιουδήποτε μεγέθους δικτυακά περιβάλλοντα, η υποστήριξη μοντέλων εμπιστοσύνης πολλά-προς-πολλά και η ευελιξία των υπηρεσιών που προσφέρει. Επιπλέον, η επιτυχημένη εφαρμογή PKI λύσεων σε ενσύρματα και τελευταία σε ασύρματα περιβάλλοντα, αποτελεί θετική παρακαταθήκη για το μέλλον.

Παρόλα αυτά, μέχρι στιγμής, οι υπεύθυνοι οργανισμοί προτυποποίησης των αρχιτεκτονικών δικτύων κινητών επικοινωνιών, άφησαν εκτός του αρχικού σχεδιασμού τους λύσεις προσανατολισμένες σε PKI. Τα βασικά τους επιχειρήματα που αιτιολογούν αυτή την απόφαση είναι ο αυξημένος υπολογιστικός φόρτος που προκαλεί η χρήση ασύμμετρων κρυπτογραφικών τεχνικών στα περιορισμένων δυνατοτήτων τερματικά των τελικών χρηστών αλλά και η επίτευξη μέγιστης συμβατότητας με τα πρότυπα των προηγούμενων γενιών. Ταυτόχρονα όμως, διάφορα ερευνητικά έργα και ομάδες έδειξαν ότι η εφαρμογή ασύμμετρων κρυπτογραφικών τεχνικών για τα συστήματα της τρίτης γενιάς είναι όχι μόνο κατορθωτή αλλά και ότι το διαφαινόμενο όφελος, τόσο για τους παρόχους όσο και για τους χρήστες, είναι σημαντικό (βλ. Κεφάλαιο 2).

Η εισαγωγή IP τεχνολογίας στα κεντρικά δίκτυα των παρόχων 2.5/3G υπηρεσιών οριοθετεί τη μετάβαση από τις υπηρεσίες φωνής στις υπηρεσίες δεδομένων. Με βάση αυτή τη διαπίστωση, τα δίκτυα των 2.5/3G παρόχων δεν πρέπει πλέον να θεωρούνται ως κλειστά αλλά αντίθετα ως ανοικτά περιβάλλοντα, ενοποιημένα με το Διαδίκτυο και τα δίκτυα άλλων παρόχων. Τούτο είναι ιδιαίτερα εμφανές στην περίπτωση του all-IP πολυμεσικού υπο-συστήματος του UMTS. Σ' αυτό το νέο πλαίσιο, το συμμετρικό μοντέλο δεν επαρκεί. Το μεγάλο πλήθος των παρόχων, οι σχέσεις που θα αναπτύσσονται μεταξύ αυτών και του Διαδικτύου, αλλά και οι ετερογενείς τεχνολογίες των δικτύων πρόσβασης (3G / 802.11 / HiPERLAN, κτλ), διαμορφώνουν νέα δεδομένα από πλευράς επιλογών ασφαλείας.

Η προσαρμογή στοιχείων PKI στα κεντρικά 3GPP δίκτυα μπορεί να βοηθήσει προς αυτή την κατεύθυνση. Μια PKI είναι δυνατό να λειτουργήσει είτε υπό την εποπτεία του εκάστοτε παρόχου (πλήρη ενσωμάτωση) είτε με τη μορφή μιας έμπιστης τρίτης οντότητας. Αν αυτό επιτευχθεί, ο πάροχος έχει στη διάθεσή του μια πλειάδα δοκιμασμένων, ισχυρών, ευέλικτων και κλιμακούμενων υπηρεσιών - πρωτοκόλλων (IKE, IPsec, SSL) ασφαλείας για να εξασφαλίσει τόσο τις ενδο-δικτυακές όσο και τις δια-δικτυακές επικοινωνιακές του ανάγκες (βλ. Κεφάλαιο 3).

Το μεγαλύτερο μειονέκτημα των 2/2.5/3G διαδικασιών αυθεντικοποίησης και συμφωνίας κλειδιού είναι ότι εξαρτώνται από την υποκείμενη τεχνολογία προσπέλασης και υποδομής δικτύου, επιλέγοντας έτσι λύσεις προσανατολισμένες στο εκάστοτε πρόβλημα (case-oriented). Εκτιμάται ότι για τα μελλοντικά συστήματα κινητών επικοινωνιών, απαιτείται περισσότερο ολοκληρωμένη προσέγγιση, προκειμένου έτσι να είναι σε θέση να υποστηρίξουν υπηρεσίες ανάλογα με τη ζήτηση (on-demand), all-IP και απ' άκρο σ' άκρο, ενοποιημένες με το Διαδίκτυο και άλλα ετερογενή περιβάλλοντα. Αλλά και σύμφωνα με την all-IP / 4G οπτική, μια «ανεξαρτήτως τεχνολογίας» προσέγγιση του ζητήματος θα ήταν ενδεχομένως καταλληλότερη.

Κατ' αυτό τον τρόπο, η διαδικασία αυθεντικοποίησης μεταξύ των χρηστών κινητών επικοινωνιών και των παρόχων των υπηρεσιών αυτών, μπορεί να θεωρηθεί ως υπηρεσία, η οποία θα εκτελείται σε υψηλότερο επίπεδο (κάτω από το επίπεδο εφαρμογής). Κατά συνέπεια έχουμε τη δυνατότητα να υλοποιήσουμε περισσότερο ασφαλείς, ευέλικτες ευπροσαρμόσιμες και ανεξάρτητες της τεχνολογίας πρόσβασης δικτύου, διαδικασίες αυθεντικοποίησης και συμφωνίας κλειδιού (Authentication and Key Agreement, AKA) για τα 3G και 4G συστήματα κινητών επικοινωνιών.

Για το συγκεκριμένο θέμα, η ερευνητική μας δραστηριότητα βασίστηκε στο γνωστό και δοκιμασμένο *de-facto* πρότυπο πρωτόκολλο SSL/TLS, προκειμένου να προτείνει και να αξιολογήσει μια διαδικασία αυθεντικοποίησης και συμφωνίας κλειδιού, η οποία εκτός των άλλων

είναι σε θέση να εκμεταλλευτεί τις υπάρχουσες υποδομές δημόσιου κλειδιού και να προστατέψει αποτελεσματικά την ιδιωτικότητα των συνδρομητών. Λαμβάνοντας υπόψη τις υψηλές ταχύτητες δικτύου που ήδη προσφέρουν τα 3G και B3G συστήματα, τις διάφορες βελτιώσεις του πρωτοκόλλου, καθώς και τις ολοένα και εντυπωσιακότερες τεχνολογικές αναβαθμίσεις στο υλικό των φορητών συσκευών, καταλήξαμε στο συμπέρασμα ότι ο προτεινόμενος AKA SSL μηχανισμός είναι σε θέση να αποτελέσει μία πραγματοποιήσιμη και αξιόπιστη επιλογή (βλ. Κεφάλαιο 4).

Πλησιάζοντας όλο και περισσότερο την προοπτική της all-IP 4^{ης} γενιάς και του ετερογενούς περιβάλλοντος που αυτή αναγγέλλει, ασχοληθήκαμε με το πρόβλημα της αυθεντικοποίησης των χρηστών που κινούνται σε ετερογενή 3GPP/WLAN περιβάλλοντα. Λαμβάνοντας υπόψη τις τρέχουσες τεχνικές προδιαγραφές της 3GPP στο συγκεκριμένο θέμα, υποστηρίξαμε ότι ο μηχανισμός EAP-TLS, υποβοηθούμενος από κατάλληλες υποδομές δημόσιου κλειδιού, είναι σε θέση να προσφέρει ευέλικτες, εύκολα κλιμακούμενες και απ' άκρο σ' άκρο λύσεις στο συγκεκριμένο πρόβλημα.

Αντιπαραβάλαμε την πρότασή μας με τον αντίστοιχο 3GPP μηχανισμό (EAP-AKA) και διαπιστώσαμε ότι το πρωτόκολλο EAP-TLS μπορεί να ξεπεράσει τις ανεπάρκειες και αδυναμίες που παρουσιάζουν οι μηχανισμοί αυθεντικοποίησης των 3G και WLAN συστημάτων, ενώ ταυτόχρονα απαιτεί ελάχιστες αλλαγές στην 3GPP αρχιτεκτονική και στον ήδη εγκατεστημένο εμπλεκόμενο δικτυακό εξοπλισμό. Εκτιμήσαμε την απόδοση του προτεινόμενου μηχανισμού σε πραγματικό περιβάλλον, χρησιμοποιώντας μια πρότυπη πειραματική διάταξη και αρκετά διαφορετικά σενάρια. Τα αποτελέσματα με τη μορφή μέσων χρόνων εξυπηρέτησης, ενισχύουν την άποψη ότι ο μηχανισμός EAP-TLS μπορεί να αποτελέσει μια αξιόπιστη και προπαντός εύκολα προσαρμόσιμη εναλλακτική λύση (βλ. κεφάλαιο 5).

Τα οφέλη από την εισαγωγή και αξιοποίηση της τεχνολογίας PKI στα δίκτυα κινητών επικοινωνιών δεν περιορίζονται μόνο στην παροχή αξιόπιστων υπηρεσιών αυθεντικοποίησης και προστασίας της ιδιωτικότητας των χρηστών, καθώς και εξασφάλισης των δια-δικτυακών και ενδο-δικτυακών επικοινωνιών των δικτύων των παρόχων. Άλλες, εξίσου σημαντικές με τις προηγούμενες, προστιθέμενης αξίας (added-value) υπηρεσίες μπορούν επίσης να υλοποιηθούν με επιτυχία και μειωμένα διαχειριστικά κόστη. Μια απ΄ αυτές είναι και η παροχή ψηφιακών πιστοποιητικών στους 3GPP συνδρομητές.

Κινούμενοι πάντα στα πλαίσια της 3G προς 4G οπτικής, προτείναμε και αναλύσαμε μια πρακτικά υλοποιήσιμη 3G-WLAN υβριδική αρχιτεκτονική, η οποία είναι πλήρως συμβατή με τις τελευταίες τεχνικές προδιαγραφές της 3GPP και μπορεί να παρέχει ψηφιακά πιστοποιητικά στους συνδρομητές ανεξαρτήτως του δικτυακού τομέα που αυτοί κινούνται. Η ιδέα μας βασίζεται σε μια νέα δικτυακή οντότητα, η οποία εισάγεται στο κεντρικό δίκτυο του 3GPP ή/και

WLAN παρόχου και λειτουργεί ως πύλη παροχής υπηρεσιών ψηφιακών πιστοποιητικών για τους χρήστες. Η ανάλυσή μας εστιάστηκε στην παροχή πιστοποιητικών ιδιοτήτων, μιας και αυτά μπορούν να παίξουν σημαντικό ρόλο σε υπηρεσίες εξουσιοδότησης των συνδρομητών, ενώ ταυτόχρονα, λόγω της προσωρινής φύσης τους, δεν απαιτούν την υλοποίηση διαδικασιών ανάκλησης. Παρόλα αυτά, το προτεινόμενο μοντέλο είναι δυνατό να χρησιμοποιηθεί ως βάση για προσφορά υπηρεσιών έκδοσης και διαχείρισης οποιωνδήποτε τύπων ψηφιακών πιστοποιητικών. Είδαμε επίσης, ότι παρόλα τα πλεονεκτήματα που παρουσιάζει το συγκεκριμένο σχήμα, πρέπει να είμαστε ιδιαίτερα προσεκτικοί σε περίπτωση υλοποίησής του. Εντοπίσαμε διάφορες απειλές που αφορούν κυρίως το απόρρητο του ιδιωτικού κλειδιού του συνδρομητή και την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων και της σηματοδοσίας του δικτύου. Πολλές απ' αυτές τις απειλές αποτελούν μεν σύνηθες φαινόμενο για τα ενσύρματα δίκτυα (π.χ. επιθέσεις μέσω του Διαδικτύου), αλλά μια νέα πραγματικότητα, που πρέπει να αντιμετωπιστεί, για τα ασύρματα

Επιπλέον, αξιολογήσαμε την αποτελεσματικότητα της προτεινόμενης αρχιτεκτονικής, χρησιμοποιώντας δύο πρότυπες δικτυακές τοπολογίες. Οι χρόνοι εξυπηρέτησης, τόσο σε δίκτυα με τεχνολογία πρόσβασης 802.11, όσο και σε GPRS, αποδεικνύουν ότι η έκδοση πιστοποιητικών για τους συνδρομητές είναι εφικτή, ενώ παράλληλα είναι σε θέση να προσφέρει ευέλικτες και κλιμακούμενες λύσεις στους 3GPP παρόχους (βλ. Κεφάλαιο 6).

Γενικά συμπεράσματα

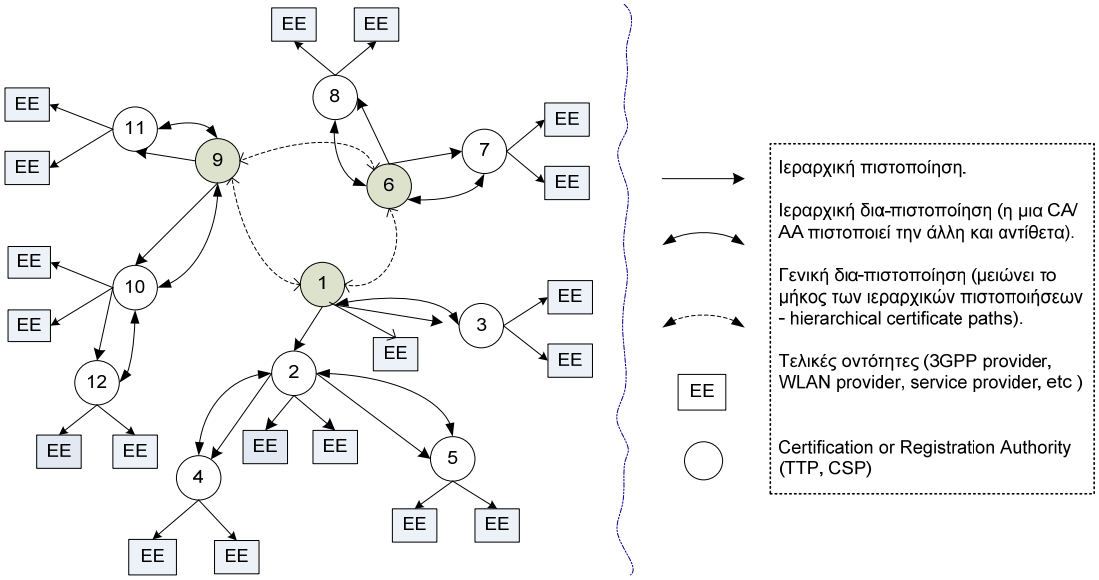
Η έρευνα που παρουσιάστηκε στην παρούσα διατριβή συνέβαλε στην:

- Ανασκόπηση και διερεύνηση των ζητημάτων ασφαλείας που εντοπίζονται στα κινητά δίκτυα επικοινωνιών τρίτης γενιάς, τόσο σε επίπεδο δικτύου όσο και σε επίπεδο χρηστών.
- Εκτίμηση και αξιολόγηση του ρόλου που μπορεί να έχει η τεχνολογία υποδομής δημόσιου κλειδιού στα δίκτυα 3G και B3G.
- Αναζήτηση μεθόδων ενσωμάτωσης της τεχνολογίας PKI στην υπάρχουσα αρχιτεκτονική-πυρήνα των δικτύων 3G.
- Αξιοποίηση της τεχνολογίας PKI για το σχεδιασμό αξιόπιστων, αποδοτικών και κλιμακούμενων 3G/B3G υπηρεσιών ασφαλείας που απευθύνονται τόσο στους συνδρομητές των δικτύων αυτών, όσο και στους αντίστοιχους παρόχους.

7.2. Προοπτικές περαιτέρω έρευνας

Η παρούσα διατριβή είχε ως στόχο να συνεισφέρει στο ζήτημα των μεθόδων ενσωμάτωσης και αξιοποίησης της τεχνολογίας PKI στα δίκτυα 3G/B3G. Εντούτοις, έχοντας πάντα κατά νου το 4G μοντέλο, δεν εξετάζει αναλυτικά τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο

θέματα που ανακύπτουν αναφορικά με τις σχέσεις εμπιστοσύνης που αναπτύσσονται μεταξύ των δικτυακών τομέων που αντιστοιχούν σε διάφορους παρόχους (inter-domain aspects). Για παράδειγμα, τι μπορεί να συμβεί αν κάποιος WLAN πάροχος δεν έχει συνάψει κάποια συμφωνία περιαγωγής με το HN του συνδρομητή; Πώς καθορίζονται οι σχέσεις εμπιστοσύνης μεταξύ των CA/AA που εκδίδουν ACs, των 3GPP και WLAN παρόχων και των παρόχων των διάφορων υπηρεσιών (service providers); Οι δια-πιστοποιήσεις (cross-certifications) μεταξύ των εμπλεκόμενων CA/AAs, όταν το μοντέλο βρίσκεται σε πλήρη ανάπτυξη, είναι αρκετές ώστε να λυθεί το συγκεκριμένο πρόβλημα; Μήπως θα πρέπει να υιοθετηθεί ένα πολυεπιπεδικό (layered) μοντέλο; Οι υπηρεσίες που αναπτύχθηκαν στα προηγούμενα κεφάλαια (AKA-SSL, EAP-TLS, ACs, κτλ) μπορούν να λειτουργήσουν το ίδιο αποδοτικά σε μια τόσο μεγάλη κλίμακα ανάπτυξης; Το σχήμα 7-1 προσπαθεί να σκιαγραφήσει και να προσεγγίσει το συγκεκριμένο ζήτημα, χρησιμοποιώντας μια υβριδική αρχιτεκτονική (Hybrid trust model). Άλλες εναλλακτικές λύσεις, όπως η χρήση γεφυρωμένων CA/AA μοντέλων (Bridge CA models) μπορούν επίσης να προταθούν. Παρόλα αυτά, συγκεκριμένες και ασφαλώς τεκμηριωμένες απαντήσεις στο συγκεκριμένο θέμα είναι δυνατό να προέλθουν μόνο από περαιτέρω έρευνα.



Σχήμα 7-1. Υβριδικό μοντέλο εμπιστοσύνης

Ένα άλλο ζήτημα που χρήζει ιδιαίτερης προσοχής και περαιτέρω διερεύνησης είναι η μελέτη του πώς ακριβώς καθορίζονται οι σχέσεις μεταξύ του HSS (το οποίο στην ουσία είναι η βάση με τα profiles των συνδρομητών) και των CA/AAs που ανήκουν ή συνεργάζονται με τον εκάστοτε 3GPP πάροχο. Για παράδειγμα, προκειμένου η CA/AA να εκδώσει το PKC ενός συνδρομητή απαιτείται κάποιου είδους επικοινωνία με το HSS του HN. Πώς ακριβώς θα γίνεται αυτό; Ποιες επιμέρους διαδικασίες απαιτούνται; Στην ενότητα 6.3, επισημαίνεται ότι ο AAA εξυπηρέτης επιστρέφει στο CGW πληροφορίες σχετικές με την έκδοση ACs από το profile του κάθε συνδρομητή που αυθεντικοποιείται. Μήπως όμως θα ήταν αποτελεσματικό-

τερο να καθοριστεί μια απευθείας διαδικασία επικοινωνίας μεταξύ CGW – CA/AA; Σε άλλες περιπτώσεις όπου απαιτείται ανάκληση των πιστοποιητικών ορισμένων συνδρομητών (μέσω του IMSI), το HSS θα πρέπει ανάλογα να ενημερώσει (;) το PKI υποσύστημα (βλ. ενότητα 4.4.1). Είναι αυτό απαραίτητο; Ή απλώς αρκεί η προσκόμιση (downloading) της λίστας με τα ανακλημένα IMSI (άρα και πιστοποιητικά) στο SGSN/GGSN;

Ένα τελευταίο αλλά εξίσου σημαντικό ζήτημα είναι η αναγνώριση και αντιμετώπιση των απειλών, οι οποίες μπορούν να προέλθουν από το παραπάνω πολυ-σχεσιακό περιβάλλον. Για παράδειγμα, όπως αναφέρθηκε στο Κεφάλαιο 2 και στην ενότητα 6.4.3, η εισαγωγή της τεχνολογίας PKI είναι σε θέση να επιλύσει και να ενδυναμώσει πολλές διαδικασίες διαδικτυακής και ενδο-δικτυακής ασφάλειας. Όμως οι πάροχοι θα πρέπει να είναι προετοιμασμένοι να αντιμετωπίσουν ένα πλήθος επιθέσεων που συναντώνται περισσότερο στα ενσύρματα δίκτυα (DoS, DDoS, Service Spoofing, Masquerading, UICC cloning, Private Key related attacks, κτλ).

Ολοκληρώνοντας, πιστεύουμε ότι η εισαγωγή τεχνολογίας PKI στα μελλοντικά συστήματα κινητών επικοινωνιών - ειδικά όσο μεταβαίνουμε προς ένα 4G ενοποιημένο περιβάλλον – είναι δυνατό να προσφέρει ουσιαστικές και αποτελεσματικές λύσεις, μερικές από τις οποίες αναπτύσσονται στην παρούσα διατριβή. Διάφορες άλλες, εξίσου αποτελεσματικές, βασισμένες σε PKI υπηρεσίες, μπορούν επίσης να προταθούν και να σχεδιαστούν προσφέροντας άμεσα πλεονεκτήματα τόσο στους συνδρομητές, όσο και στους 3GPP παρόχους.

Βιβλιογραφία

3GPP Technical Specification (2000). *A guide to 3rd Generation Security*, TS 33.900 v.1.2.0, Jan 2000.

3GPP Technical Specification (2002). *MAP Application Layer Security*, TS 33.200 v.5.1.0, Dec. 2002.

3GPP Technical Specification (2002b). *Access Security for IP-based services*, TS 33.203 v.5.2.0, June 2002.

3GPP Technical Specification (2002c). *Security Architecture*, TS 33.102 v.5.1.0, Dec. 2002.

3GPP Technical Specification (2002d). *WLAN interworking Security*, TS 33.cde v.0.1.0, July 2002.

3GPP Technical Specification (2003). *Network Architecture*, TS 23.002, v. 6.2.0, Sep. 2003.

3GPP Technical Specification (2003b). *3GPP system to WLAN interworking*, TS 24.234 v.0.2.0 Release 6, Nov. 2003.

3GPP Technical Specification, (2003c). *Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description*, TS ab.cde v.0.3.0, Sept. 2003.

3GPP Technical Specification, (2004). *3GPP system to WLAN Interworking; System description*, TS 23.234 v.6.1.0, June 2004.

3GPP Technical Specification, (2004b). *3GPP System to WLAN Interworking; UE to Network protocols*, TS 24.234 v.1.5.0, July 2004.

3GPP Technical Specification, (2004c), *WLAN Interworking Security*, TS 33.234 v.6.1.0, June 2004.

3GPP Technical Specification, (2004d). *Generic Authentication Architecture (GAA); Support for subscriber certificates*, TS 33.221 v.6.0.0, March 2004.

3GPP Technical Specification, (2004e). *IP Network Layer Security*, TS 33.210 v.6.5.0, June 2004.

3GPP TSG (2001). *Using PKI to provide network domain security*, discussion document, (S3-010622 SA WG3 Security- S3#15bis), Nov. 2001.

3GPP TSG (2001a). *Support of certificates in 3GPP security architecture*, discussion document S3-010353 SA WG3 Security – S3#19, July 2001.

3GPP TSG (2002). *Architecture proposal to support subscriber certificates*, discussion and approval document, Tdoc S2-022854, Oct 2002.

3GPP TSG (2002b). *LS on subscriber certificates*, discussion document S3-020597, Tdoc S2-023130 SA WG3 Security – S3#26, Release 6, Oct 2002.

3GPP TSG (2004). *3GPP2 Security – Report to 3GPP",* SA WG3 (Security) meeting, S3-040588, Acapulco, Mexico, July 2004.

3GPP2 TSG (2004). *3GPP2 System to Wireless Local Area Network Interworking,* TSG-X/TIA TR-45.6, to be published as 3GPP2 X.S0028.

Aamodt, T., Fruso, T. and Koien, G. (2001). *Security in UMTS – Integrity*, Telenor R&D, Norway.

Aboba, B. and Beadles, M. (1999). *The Network Access Identifier*, IETF RFC 2486, January 1999.

Aboba, B. and Simon, D. (1999). *PPP EAP TLS Authentication Protocol*, IETF RFC 2716, Oct. 1999.

Adams, C. & Lloyd, S. (1999). *Understanding Public-Key Infrastructure, Concepts, Standards and Deployment Considerations*, Indianapolis, IN: New Riders.

Adrangi, F. (Editor), (2004). *Mediating Network Discovery and Selection*, IETF RFC, <draft-adrangi-eap-network-Discovery-and-Selection-01.txt>, Feb. 2004.

Al-Muhtadi, J. Mickunas, D. and Campbell, R. (2002). A lightweight reconfigurable security mechanism for 3G/4G mobile devices, *IEEE Wireless Communications*, **9**(2), pp. 60-65.

Apostolopoulos, G., Peris, V., Pradhan, P. and Saha, D. (2000). Securing electronic commerce: reducing SSL overhead, *IEEE Network Magazine*, **14**(4), pp. 8-16.

Arkko, J. and Blom, R. (2004). *The Mobile Application Part SECurity (MAPSEC) Domain of Interpretation (DOI) for the Internet Security Association and Key Management Protocol (ISAKMP)*, IETF Internet Draft, <draft-arkko-map-doi-07.txt>, March 2004.

Arkko, J. and Haverinen, H. (2003). *EAP-AKA authentication*, IETF Draft <draft-arkko-pppext-eap-aka-11.txt>, Oct. 2003.

Arseanult, A and Turner, S. (2002). *Internet X.509 Public Key Infrastructure: Roadmap*, PKIX Working Group, IETF Internet Draft, <draft-ietf-pkix-roadmap-09.txt>, July 2002.

Asokan, N., Valtteri, N. and Nyberg, K. (2002). *Man-in-the-middle in Tunnelled Authentication*, Nokia Research Centre.

ASPeCT Project (1999). *Securing the future of Mobile Communications*, electronically available at:http://www.esat.kuleuven.ac.be/cosic/aspect.

Assaf, N., Luo, J., Dillinger, M. and Menendez, L. (2002). Interworking between IP security and Performance Enhancing Proxies for Mobile Networks, *IEEE Communications Magazine*, **40**(5), pp. 138-144.

Biryukov, A. and Shamir, A. (1999). *Real-Time Cryptanalysis of the Algorithm A5/1 on a PC*, preliminary Draft.

Boyd, C. and Mathuria, A. (2003). *Protocols for Authentication and Key Establishment*, Springer–Verlag.

Burnside, M., Clarke, D., Mills, T., Maywah, S., Devadas, S. and Rivest, R. (2002). Proxy-based Security Protocols in Networked Mobile Devices, in *Proceedings of ACM SAC 2002 Int'l Conference*, Madrid, Spain, pp. 265-272.

Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and Arkko, J. (2003). *Diameter Base Protocol*, IETF RFC 3588, Sep. 2003.

Chadwick, D. (2002). The *PERMIS X.509 Based Privilege Management Infrastructure*, IETF Internet Draft, <draft-irtf-aaaarch-permis-00.txt>, Apr. 2002.

Chakravorty, R. and Pratt, I. (2002). Performance Issues with General Packet Radio Service, *Journal of Communications and Networks (JCN), Special Issue on Evolving from 3G deployment to 4G definition*, **4**(2), pp. 266-281.

Chankravorty, R., Cartwright, J. and Pratt, I. (2002). Practical Experience with TCP over GPRS, in *Proceedings of the IEEE GLOBECOM*, Taipei, Taiwan.

Chen, H., Zivkovic, M. and Plas, D. (2003). Transparent end-user authentication across heterogeneous wireless networks, in *Proceedings of IEEE Int'l Conference in Vehicular Technology (VTC)*, Seoul, Korea.

Dierks, T. and Allen, C. (1999). *The TLS Protocol Version 1.0*, IETF RFC 2246, Jan 1999.

Diffie, W. and Hellman, M. (1976). New Directions in Cryptography, *IEEE Transactions on Information Theory*, **22**, pp. 644-654.

Dixit, S. and Prasad, R (eds.). (2004). *Wireless IP and Building the Mobile Internet*, Artech House.

Eaton, D. (2003). *Diving into the 802.11i spec: A tutorial*, electronically available at: http://www.commsdesign.com/design_corner/OEG20021126S0003.

eNorge 2005 project (2002). Naerings – og handelsdepartementet.

Farrell, S. and Housley, R. (2002). An *Internet Attribute Certificate Profile for Authorization*, IETF RFC 3281, April 2002.

Ferraiolo, D.F, Cugini, D.A. and Kuhn, R.D. (1995). *Role-Based Access Control (RBAC): Features and Motivations*, available at: http://hissa.ncsl.nist.gov/rbac/newpaper /rbac. html, 1995.

Frankel, S. (2001). *Demystifying IPsec Puzzle*, Artech House.

Frier, A., Karlton, P. and Kocher, P. (1996). *The SSL 3.0 Protocol Version 3.0*, electronically available at: http://home.netscape.com/ssl3/draft302.txt.

Frodigh, M., Parkvall, S., Roobol, S., Johansson, P. and Larsson, P. (2001) Future-Generation Wireless Networks, *IEEE Personal Communications Magazine*, **8**(5), pp. 10–17.

Funk, P. and Blake-Wilson, S. (2002). *EAP Tunnelled TLS Authentication Protocol (EAP-TTLS)*, IETF Internet Draft, <draft-ietf-pppext-eap-ttls-01.txt>, Feb. 2002.

Gast, M. (2002). *802.11 wireless networks: The definitive guide*, O'Reilly & Associates.

Grecas, C., Maniatis, S. and Venieris, I. (2003). Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and its Public Key Infrastructure Integration, *Journal of Mobile Networks and Applications*, Elsevier Science, **8**(3), pp. 145-150.

Gupta, V. and Gupta, S. (2002). Experiments in Wireless Internet Security, in *Proceedings of IEEE wireless Communications and Networking Conference (WCNC)*, pp. 859-863.

Hahnsang, K. and Hossam, A. (2003). Improving mobile authentication with new AAA protocols, in *Proceedings of the IEEE int'l Conference Communications (ICC)*, **1**, pp. 497-501.

Harbitter, A. and Menasce, D. (2001). The performance of public key-enabled authentication in mobile computing applications, in *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS-8)*, Philadelphia, USA, pp. 78-85.

Housley, R. and Polk, T. (2001). *Planning for PKI*, John Wiley and Sons.

IEEE Std 802.11 (1999). *Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, IEEE, Sep. 1999.

IETF PKIX working Group (2004). *Public-Key Infrastructure (X.509)*, PKIX-charter, currently available at: http://www.ietf.org/html.charters/pkix-charter.html.

Iliadis, J., Gritzalis, S., Spinellis, D., De Cock, D., Preneel, B. and Gritzalis, D. (2003). Towards a Framework for Evaluating Certificate Status Information Mechanisms, *Computer Communications*, **26**(16), pp. 1839-1850, Elsevier Science.

ITU-R Draft Rec. M. (2000). *Detailed specifications of the Radio Interfaces of IMT-2000*, Doc 8/126.

ITU-T Recommendation X.509. (1997). *Information Technology-Open Systems Interconnection - The Directory: Authentication Framework*, (equivalent to ISO/IEC 9594-8, 1997), 1997.

Kambourakis, G., Rouskas, A. and Gritzalis, S. (2002). Using SSL in Authentication and Key Agreement Procedures of Future Mobile Networks, in *Proceedings of the 4th IEEE Int'l Conference on Mobile and Wireless Communication Networks (MWCN)*, Stockholm, Sweden, pp. 152-156.

Kambourakis, G., Rouskas, A. and Gritzalis, S. (2003). Introducing PKI to enhance security in future mobile networks, in *Proceedings of the IFIPSEC'2003 18th int'l Security Conference*, pp. 109-120, Athens, Greece.

Kambourakis, G. Rouskas, A. and Gritzalis, S. (2004). Inter/Intra Core Network Security with PKI for 3G-and-Beyond Systems, in *Proceedings of the 3rd IFIP TC-6 Int'l Conference on Networking (NETWORKING '04)*, pp. 13-24, May 2004, Athens, Greece, Lecture Notes in Computer Science LNCS, Springer.

Kambourakis, G., Rouskas, A. and Gritzalis, S. (2004b). Delivering Attribute Certificates over GPRS, in *Proceedings of the 19th ACM Symposium on Applied Computing (SAC'04) – Mobile Computing and Applications Track*, pp. 1166-1170, Nicosia, Cyprus, ACM Press.

Kambourakis, G., Rouskas, A. and Gritzalis, S. (2004c). Performance Evaluation of Public Key-based Authentication on Future Mobile Networks, *EURASIP Journal on Wireless Communications and Networking (JWCN)*, **1**, pp. 184-197.

Kambourakis, G., Rouskas, A. and Gritzalis, S. (2004d). Experimental Analysis of an SSL-based AKA Mechanism in 3G-and-Beyond Wireless Networks, *Journal of Wireless Personal Communications (WPC), special issue on security for next generation communications,* Kluwer, accepted for publication, April 2004.

Kambourakis, G., Rouskas, A., Kormentzas, G. and Gritzalis, S. (2004e). Advanced SSL/TLS-based authentication for Secure WLAN-3G Interworking, *IEE Proceedings Communications*, accepted for publication, June 2004.

Kambourakis, G., Rouskas, A., Gritzalis, S. and Geniatakis, D. (2004g). Support of Subscribers' Certificates in a Hybrid WLAN-3G Environment, Submitted for publication in *Computer Networks*, Elsevier Science, Ref. Number COMNET-D-04-00623.

Kambourakis, G., Kontoni, D.-P., Rouskas, A. and Gritzalis, S. (2004h). A PKI Approach for Deploying Modern Secure Distributed e-learning and m-learning Environments, *Computers & Education*, Elsevier Science, accepted for publication, Oct. 2004.

Karri, R and Mishra, P. (2002). Minimization of Energy Consumption of Secure Wireless Session with QOS Constraints, in *Proceedings of IEEE Int'l Conference on Communications*, New York, USA.

Kaufman (editor) (2004). *Internet Key Exchange (IKEv2) Protocol*, IETF Internet Draft <draft-ietf-ipsec-ikev2-13.txt>, March 2004.

Kent. S. and Atkinson, R. (1998). Security *Architecture for the Internet Protocol*, IETF RFC 2401, Nov. 1998.

Khare, R. (1999). W* Effect Considered Harmful, *IEEE Internet Computing*, **3**(4), pp. 82-92.

Koien, G. (2004). An Introduction to Access Security in UMTS, *IEEE Wireless Communications Magazine*, **11**(1), pp. 8-18.

Koien, G. and Haslestad, T. (2003). Security Aspects of 3G-WLAN Interworking, *IEEE Communications Magazine*, 2003, **41**(11), pp. 82-88.

Korhonen, J., Aalto, O., Gurtov, A. and Laamanen, H. (2001). Measured Performance of GSM, HSCSD and GPRS, in *Proceedings of the IEEE Int'l Conference on Communications (ICC)*, Helsinki, Finland.

Lin, Y., Pang, A., Haung, Y. and Chlamtac, I. (2002). An All-IP Approach for UMTS Third-Generation Mobile Networks, *IEEE Network Magazine*, **16**(5), pp. 8-19.

Maughan, D., Schertler, M., Schneider, M. and Turner, J. (1998). *Internet Security Association and Key Management Protocol (ISAKMP)*, IETF RFC 2408, Nov. 1998.

Nachiketh, R., Srivaths, R., Raghunatan, A. and Niraj, J. (2003). Analysing the Energy Consumption of Security Protocols, in *Proceedings of ACM ISPLED Conference*, Seoul, Korea, pp. 30-35.

Nash, A., Duane, W., Joseph, C. & Brink, D. (2001). *PKI Implementing and Managing E-Security*, Berkeley: RSA press.

Niemi, V. and Nyberg, K. (2004). *UMTS Security*, John Wiley & Sons.

Oppliger, R. (2000). *Security Technologies for the World Wide Web*, Artech House, Boston, Mass, USA, 2000.

Oppliger, R. (2002). *Internet and Intranet Security*, 2nd Edition, Artech House.

Oppliger, R., Pernul, G. and C. Strauss, Using Attribute Certificates to Implement Role Based Authorization and Access Control Models, in the *Proc. of 4. Fachtagung Sicherheit in Informationsystemen (SIS 2000)*, Zurich, Switzerland, 169 – 184, 2000.

Otenko, S. and Chadwick, D. (2003). *A Comparison of the Akenti and PERMIS Authorization Infrastructures*, version 2.1, July 2003, electronically available at: http://esc.isi.salford.ac.uk/download/AkentiPERMISDeskcomparison2-1.pdf.

Palekar, A., Simon, D., Salowey, D., Zhou, H., Zorn, G. and Josefsson, S. (2004). *Protected EAP Protocol (PEAP) Version 2*, IETF Internet Draft, <draft-josefsson-pppext-eap-tls-eap-08.txt>, July 2004.

Patel, G. and Dennett, S. (2000). The 3GPP and 3GPP2 Movements Toward an All-IP Mobile Network, *IEEE Personal Communications Magazine*, **7**(4), pp. 62-64.

Peikari, C. and Fogie. S. (2003). *Wireless Maximum Security*, IN, Indianapolis, SAMS Publishing.

Potlapally, N., Ravi, S., Raghunathan, A. and Lakshminarayana, G. (2002). Optimizing public-key encryption for wireless clients, in *Proceedings of IEEE Int'l Conference on Communications (ICC)*, 2, pp. 1050-1056, NY, USA.

Rescorla, E. (2001). *SSL and TLS Designing and Building Secure Systems*, Addison-Wesley.

Rescorla, E. (1999). *Diffie-Hellman Key Agreement Method*, IETF RFC 2631, June 1999.

Rigney, C., Willens, S., Rubens, A. and Simpson, W. (2000). *Remote Authentication Dial In User Service (RADIUS)*, IETF RFC 2865, June 2000.

Rivest, R. L., Shamir, A. and Adleman, L. M. (1978). A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, **2**(21), pp. 120-126.

Rose, G. and Koien, G. M. (2004). Access Security in CDMA2000, including a comparison with UMTS Access Security, *IEEE Wireless Communications Magazine*, **11**(1), pp. 19-25.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E. (2002). *SIP: Session Initiation Protocol*, IETF RFC 3261, June 2002.

Rossnagel, H. (2004). Mobile Qualified Electronic Signatures and Certification on Demand, in *Proceedings of the 1st European PKI Workshop*, Samos Greece, pp. 274-286.

Salkintzis A., Fors, A. and Pazhyannur, R. (2002). WLAN-GPRS integration for next-generation mobile data networks, *IEEE Wireless Communications*, **9**, pp. 152-156.

Salsano, S., Veltri, L. and Papalilo, D. (2002). SIP Security Issues: The SIP Authentication Procedure and its Processing Load, *IEEE Network Magazine*, **16**(6), pp. 38-44.

Thomas, S. (2000). *SSL and TLS essentials: Securing the Web*, John Wiley and Sons.

Thompson, M., Johnston, W., Mudumbai, S., Hoo, G., Jackson, K., and A. Essiari, A. (1999). Certificate-based Access Control for Widely Distributed Resources, In *Proceedings of the 8th USENIX Security Symposium*, Washington, D.C.

Tiller, J. (2000). *A Technical Guide to IPsec Virtual Private Networks*, Auerbach CRC Press.

Trask N. T. and Jaweed, S. A. (2001). Adapting public key infrastructures to the mobile environment, *BT Communications Technology Journal*, **19**(3), pp. 76-80.

USECA Project (1999). *UMTS Security Architecture: Intermediate report on PKI architecture for UMTS*, Public report.

Viega, J., Messier, M. and Chandra, P. (2002). *Network Security with OpenSSL*, O' Reilly.

Wahl, M., Howes, T. and Kille, S. (1997). *Lightweight Directory Access Protocol (LDAP v3)*, IETF RFC 2251, Dec. 1997.

WAP Forum (2001). *Wireless PKI*, available at: http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf.

Wisely, D., Eardlay, P. and Burness, L. (2002). *IP for 3G*, Wiley.

Xenakis, C. and Merakos L. (2004). Security in third Generation Mobile Networks, *Computer Communications, Elsevier Science*, **27**, pp. 638-650.