

Mobility and Key Management in SAE/LTE

Anand R. Prasad¹, Julien Laganier¹ and Alf Zugenmaier¹
Mortaza S. Bargh², Bob Hulsebosch² and Henk Eertink²
Geert Heijenk³ and Jeroen Idserda³

¹DoCoMo Communications Labs Europe GmbH, Germany

²Telematica Instituut, The Netherlands

³Twente University, The Netherlands

Summary: Often in wireless communications the cryptographic algorithm is considered as ‘the security solution’ but actually it is only the nucleus. The means for using the cryptographic algorithm is the ‘key’ used by the algorithm. Thus management of keys and security there-of is an important issue. The security of the key management solution should not impede mobility of devices by adding undue delays. Thus, secure and fast key management during mobility is an important issue for the third generation partnership project (3GPP) activity on system architecture evolution / long-term evolution (SAE/LTE). In this paper we review mobility and security issues with the focus of key management in SAE/LTE and present possible existing solutions together with their analysis.

1. Introduction

At times, it is said that security is the holy grail of any communications system. True or false, practice shows that solutions developed without security in mind from the beginning leads to solutions that have severe issues in due course. To avoid such situations it was necessary that the third generation partnership project (3GPP) activity on their system architecture evolution and long term evolution (SAE/LTE) includes security from the very beginning. The first step for SAE/LTE activity was taken in 2004 and it is expected that the specifications will be available around September 2007. Details of 3GPP time-plan and specification can be found in [1].

The SAE part of the 3GPP activity focuses on the core network (CN) of a mobile network and the LTE part focuses on the radio access network (RAN). SAE assumes the core network will be migrated to IP as the basis communication protocol. SAE allows integration of radio access networks based on different radio access technologies into the network, e.g., UMTS, LTE, wireless LAN and WiMAX. LTE specifies a radio access technology (RAT) that is aimed at peak data-rates of 100 Mbps downlink and 50 Mbps

uplink. The goal of both SAE and LTE is also to decrease the overall complexity and cost for both operators and end-users. The security goal of the SAE/LTE activity was to provide security that is at least of the level of UMTS today. Of course, the security measures should not impede mobility support that is the essence of a mobile operator's business.

Looking at the security aspect, of the three common security goals confidentiality, integrity and availability, the first two are achieved using cryptography, which in turn requires keys to function. Key management includes key establishment and key distribution besides key generation and key management policies. The usage of the system defines the requirements for the keys. An insecure key management solution can lead to leakage of keys that can cause attack on the system or network. In such a situation the strength of the cryptographic algorithm is irrelevant.

It is of utmost importance that the mobile network is able to provide fast handovers such that there is no impact on perceived service quality by the user. These handovers need to consider security too. It should not happen that a mobile user hooks up to a rogue base station or there is hijack of the session by an intruder. This means that mobility related security requirements should be fulfilled, which includes re-keying when the user moves. Re-keying is also part of the key management and should fulfil the related requirements.

In this paper we will first discuss LTE and SAE development by 3GPP and their goals in Section 2 and 3 respectively. Possible mobility and key management related solutions are discussed in Sections 4 and 5 with an analysis and comparison of the solutions in Section 6 leading to the conclusions in Section 7.

2. Long Term Evolution

LTE or the Evolved UMTS Terrestrial Radio Access (E-UTRA) and Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) aims at developing standards that will ensure competitiveness of 3GPP in long-term (10 years or more). There are several scenarios for LTE deployment, but at a high-level one could expect two scenarios [2]. The first one is the standalone deployment and the second scenario is integration and handover with UTRAN and/or GERAN. Further it is expected [1] that in LTE there will be support for (1) shared networks during mobility and initial access, (2) various cell sizes and planned or ad-hoc deployments, and (3) efficient mobility with an intra-LTE handover interruption time of 30ms. An overview of LTE is given in this section [2-4].

Table 1 LTE major requirements.

1	Bandwidth (MHz)	Scaleable bandwidths of 1.25, 2.5, 5, 10, 15, 20
2	Data rate (Mbps)	Peak of 100 Mbps for downlink (5bps/Hz) 50 Mbps for uplink (2.5bps/Hz) at 20 MHz, with 2 Rx antennas and 1 Tx antenna at the terminal.
3	Latency (ms)	C-plane 100ms for camped to active state and 50ms between active and dormant state. Transit time between IP layers of UE and RAN less than 5 ms.
4	Capacity (users/cell)	C-plane 200 users/cell in active state for 5 MHz and at least 400 users for higher spectrum allocation. Much higher for dormant and camped state.
5	Throughput	Compared to Rel 6 average user throughput per MHz: downlink 3-4 times and uplink is 2-3 times
6	Mobility	Optimized for 0 – 15 kmph. High performance for 15 – 120 kmph. Support upto 350 kmph or 500 kmph. Rel 6 voice and real-time CS services provided over PS in LTE with interruption time less than or equal to CS domain handovers in GERAN.
7	QoS	End-to-end QoS shall be supported. VoIP with at least as good radio and backhaul efficiency and latency as voice traffic over the UMTS CS.

2.1 Requirements

Some of the major requirements for LTE are given in Table 1 [2,10].

Although the concern of cost for operators is addressed in the requirements there is no mention about security. Further the requirements set for handover with legacy solution does not allow seamless perception of service [6].

2.2 Physical Layer Parameters

Details of current work on physical layer can be found in [7]. In brief, the downlink (DL) part of LTE uses orthogonal frequency division multiplexing OFDM in which the data is multiplexed onto a number of subcarriers. This number scales with bandwidth. There is frequency selective scheduling in DL (i.e. OFDMA) and adaptive modulation and coding (up to 64-QAM). In the uplink SC-FDMA (Single Carrier - Frequency Division Multiple Access) is used with fast Fourier transform-based transmission scheme like OFDM. The total bandwidth is divided into a small number of frequency blocks to be assigned to the UEs (e.g., 15 blocks for a 5 MHz bandwidth). Multiple antenna are used (2 at eNodeB and 2 receive antennas at UE) for beam-forming and multiple input- multiple output (MIMO).

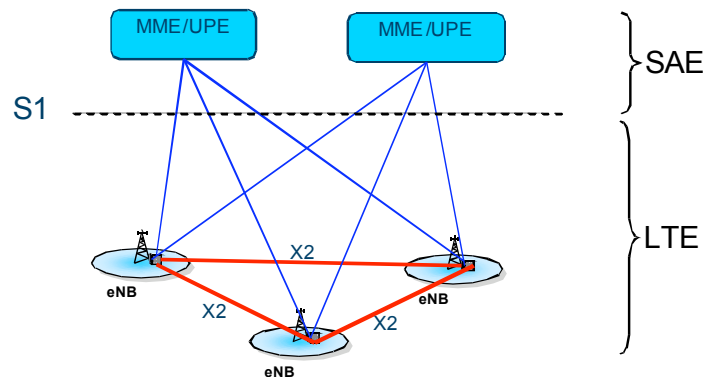


Figure 1: LTE architecture.

2.3 Architecture

The LTE architecture interconnects the network side termination points of the wireless link (called eNodeBs, eNBs) with each other, The interface for this is called X2 interface [2]. The eNBs are also connected by means of the S1 interface to the core network called Evolved Packet Core (EPC). This EPC includes Mobility Management Entities (MME) and User Plane Entities (UPE) together also known as access gateway (aGW). The LTE architecture is illustrated in Figure 1. The LTE architecture differentiates between user plane U-plane (carrying the user's applications generated traffic, e.g., voice, mail, web, etc.) and control plane C-plane (carrying the terminal's signalling protocols traffic, e.g., paging, call set-up, etc.). The U-plane and C-plane protocol stack are shown in Figure 2.

The eNB hosts the radio resource management unit that includes radio bearer control, radio admission control, connection mobility control, and dynamic resource allocation (scheduling) functions. The S1-C (control plane) interface supports, among others, intra- and inter-system mobility of UE; and the S1-U (user plane) interface supports the tunneling of end user packets between the eNB and the UPE as a means to minimize packet losses due to e.g. mobility. The X2-C interface supports UE mobility between eNBs. The X2-U interface supports the tunneling of end user packets between the eNBs as a means to minimize packet losses due to e.g., mobility.

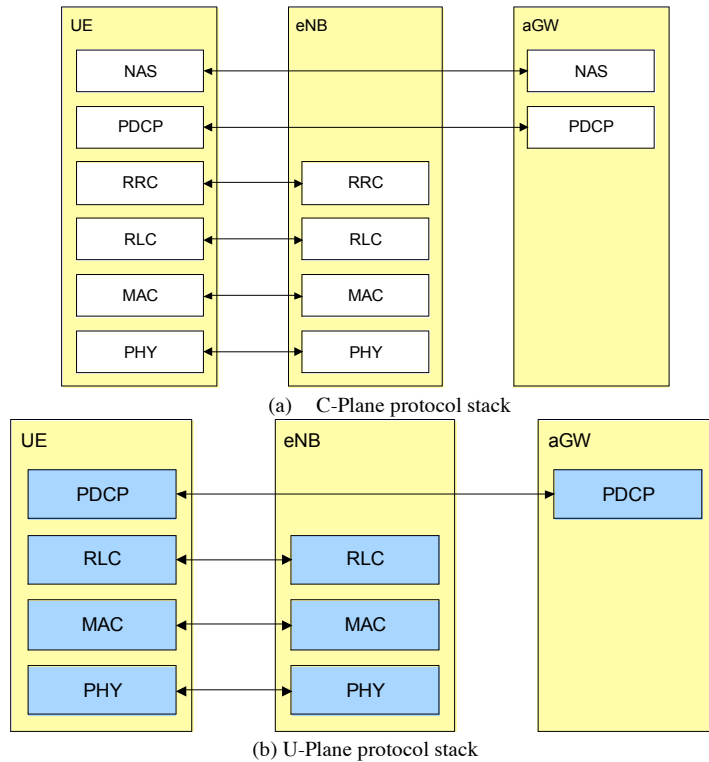


Figure 2: C-Plane and U-Plane protocol stacks.

There are several handover scenarios for LTE, dependent on the state of the mobile device, C-plane or U-plane handover, and whether the MME/UE is involved. In terms of security the RAN and security group specifications [8,9] discuss the termination point that is naturally dependent on the end-point of a given protocol. The Non Access Stratum (NAS) signalling requires confidentiality and integrity protection. U-plane must be confidentiality protected (between UE and eNB), but it is still under study whether or not its integrity shall be protected. For Access Stratum (AS) signalling, MAC security and requirement for confidentiality protection of RRC signalling is yet to be studied, while RRC signalling integrity protection is required.

3. System Architecture Evolution

System architecture evolution SAE focuses on enhancing the capability of the 3GPP system's core network to cope with the rapid growth in IP data

traffic. This 3GPP system enhancement includes reduced latency, higher user data rates, improved system capacity and coverage, and reduced overall cost for the operator. IP based 3GPP services will be provided through various access technologies together with mechanisms to support seamless mobility between heterogeneous access networks. In this section the current work of 3GPP regarding SAE are presented from [10 – 14].

3.1 Requirements

The main objectives to address are [14]:

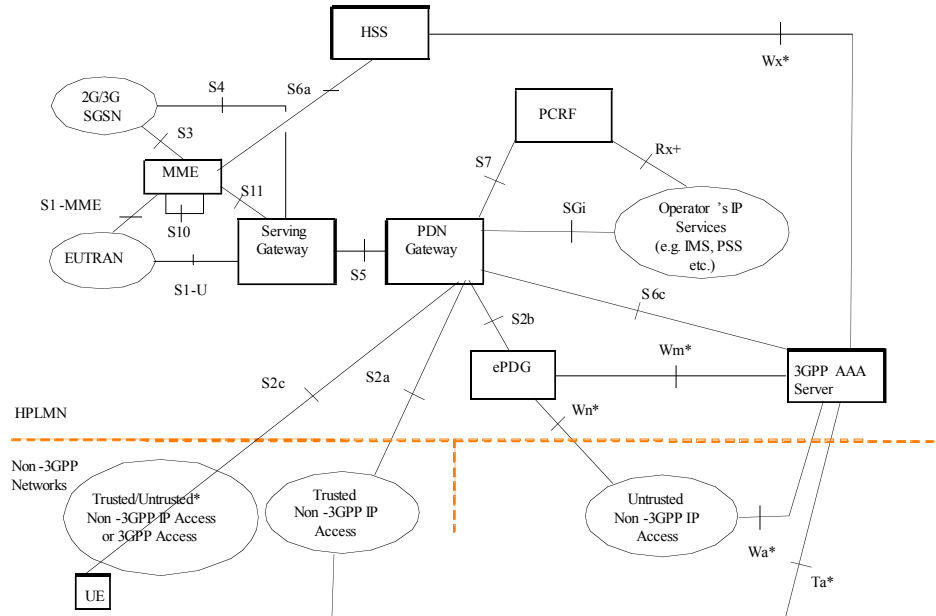
1. The architectural developments should take into account the LTE targets for the evolution of the radio-interface. It should address efficient support of services especially from the PS domain (e.g. VoIP).
2. Overall architecture impacts from support of different RAN/RATs and access selection based on combinations of operator policies, user preferences and RAN conditions; improving the basic system performance e.g. communication delay; maintaining the negotiated QoS across the whole system; etc. [12]12.
3. Overall architecture aspects of supporting mobility between heterogeneous RANs (including service continuity in PS domain); how to maintain and support the same capabilities of access control (authentication, authorization); and privacy and charging between different RATs.
4. Migration aspects should be taken into account for the above, i.e. how to migrate from the existing architecture.

3.2 Architecture

It was decided in 3GPP to proceed with two specifications; one that utilizes the existing protocol (i.e., GPRS transport protocol GTP [10]), and the other that is based on IETF solutions [11]. SAE also sets a few high level architectural principles in [4,15] A few principles regarding security and mobility are: subscriber security procedures in SAE/LTE shall assure at least the same level of UMTS security; access to network should be possible using Release 99 UMTS subscriber identity module USIM; authentication framework should be independent of the RAT; mobility management should not degrade security.

The architecture for non-roaming case is given in Figure 3. Due to lack of space only a brief explanation of network elements and interfaces is given in this section: The MME provides NAS signalling and its security,

inter CN node signalling for mobility between 3GPP access networks, etc. The Serving GW is the gateway which terminates the interface towards



* Untrusted non -3GPP access requires ePDG in the data

Figure 3: Non-roaming architecture for SAE

E-UTRAN. For each UE, at a given point of time, there is a single Serving GW with the function of Local Mobility Anchor point for inter-eNB handover, mobility anchoring for inter-3GPP mobility, lawful Interception, packet routing and forwarding. The PDN GW functions include policy enforcement, per-user packet filtering, charging support, lawful interception and UE IP address allocation.

There are several different mobility management concepts in SAE which are dependent not only on the access technology and network layer protocols but also on the state of the UE. Other mobility issues that SAE has to cater for are inter-RAT mobility, dependence of paging/tracking area, context information availability, power saving, etc.

4. Mobility Solutions

There are several network layer mobility protocols that could be utilized in SAE/LTE to support mobility within LTE and to/from other RANs. We

now know that 3GPP has made a choice of protocols. Anyhow in this section we present the different choices that were possible together with their differences and similarities. In latter section we give an analysis.

In traditional IP networks, the IP address of a node is usually bound to its topological location within the network to permit route aggregation. For a mobile node, that means that moving and changing its location implies that it changes its IP address. In the traditional TCP/IP communications paradigm, IP addresses of a node were expected to remain stable. It was thus possible to: (a) reach an IP node knowing only its IP address, (b) bind upper layer communications (e.g. TCP conations) to IP addresses of communication endpoints. With the advent of mobile nodes, this change of IP address role has thus the following implications:

1. It is no longer possible to reach a mobile node knowing only its IP address since it changes when the mobile node moves.
2. Upper layer communications will break with movement of one of the communication endpoint since they are bound to IP addresses that will change.

Because of that, network layer mobility protocols have been designed to restore the two basic properties that were broken by apparition of mobile nodes. In addition, these protocols might, depending on their architecture and mechanisms, offer additional mobility-related functionalities such as:

- Route optimisation between a mobile node and its correspondent nodes.
- Reduction of communication disruption latency upon movement via pro-active configuration of care-of address before movement, buffering of packet received at old access router (AR) and tunnelling to new AR, and/or local anchoring.
- Reduction of packet loss upon movement via pro-active configuration of care-of address before movement, buffering of packet received at old access router (AR) and tunnelling to new AR, and/or local anchoring.

Additionally, these protocols may also offer functionalities which are not directly related to mobility such as:

- Network layer multi-homing: Ability to switch between different provider-assigned subnet prefixes to cope with ISP failures. Such prefixes might be assigned on a single interface, or each prefix to a different interface.
- Network layer security: Ability to protect integrity and confidentiality of communications.

With the focus on IPv6 the protocols given below were considered in this paper for which a comparison is given in Table 2.

- Mobile IP version 6 (MIPv6)

- Fast Handover for Mobile IP version 6 (FMIPv6)
- Hierarchical Mobile IP version 6 (HMIPv6)
- Network-based Localized Mobility (NETLMM)
- IKEv2 Mobility and Multi-homing Protocol (MOBIKE)
- Host Identity Protocol (HIP)

Table 2 Differences in the mobility protocols.

	MIPv6	MIPv6 + FMIPv6	HMIPv6	HMIPv6 + FMIPv6	NETLMM	MOBIKE	HIP
Scope of Mobility	Global, Local	Global, Local	Local	Local	Local	Global, Local	Global
Location of Rendezvous point	On routing path to home address	On routing path to home address	On routing path to regional care-of-address	On routing path to regional care-of-address	On routing path to regional care-of-address	On routing path to IPsec inner address	Anywhere
Trust model	SA with rendezvous point	SA with rendezvous point	SA with rendezvous point	SA with rendezvous point	SA with access router	SA with rendezvous point	SA with rendezvous point and correspondent node
Route Optimization	Yes	Yes	No	No	No	No	Required
Reduction of communication disruption latency and packet loss.	Yes if Local Anchor	Yes	Yes	Yes	Yes	Yes if Local anchor	No
Rendezvous Point	Home Agent (HA)		Mobility Anchor Point (MAP)		Localized Mobility Anchor (LMA)	Security Gateway (SGW)	Rendezvous Server (RVS)
Routing Update	Binding Update (BU)		Local Binding Update (LBU)		Routing Update (RU)	Update SA Address (USA)	Locator Update (UPD)

5. Key Management Solutions

Authentication process is one of the major latency sources that prevents seamless handovers. This latency is mainly due to the signalling overhead that is needed to authenticate a user and for making the association with the new Access Point (AP) secure. Both aspects involve proper key management. Therefore, solutions for fast authentication are dearly needed in order to realize seamless handovers and thereby to improve the user's ex-

perience. These solutions boil down to effective and efficient key management schemes that are suitable for intra- and inter-domain handovers as well as for horizontal and vertical handovers.

The Extensible Authentication Protocol (EAP) [16] is a generic framework for network access authentication. The EAP framework allows an authenticator to authenticate a peer (and possibly mutual authentication) and establishes between them two keys, the Master Session Key (MSK) and the Extended MSK (EMSK), which are used to secure communications of EAP lower layers. At the moment only the MSK is used by different lower layers and protocols. The most common usage is in the IEEE 802.11i lower layer to derive the Transient Session Key (TSK) to provide access link security. For instance in 802.11i the first 512 bits of the MSK are used for TSK derivation, 802.11r uses the second 256 bits to derive Pair-wise MKs (PMKs-R1) for fast BSS transition, and 802.16 uses the first 320 bits. The Internet Key Exchange protocol (IKEv2) has an authentication mode where one of the IKE peer is authenticated via EAP, thus making use of the MSK as well. IKEv2, however, uses it for entity authentication purposes. This disparate usage of the MSK makes it less suitable for a root key of a key hierarchy that supports fast re-authentication for seamless handovers. For this reason, the IETF HOKEY working group tries to define an EMSK-based key hierarchy for authenticated seamless handovers [17]. Since the EMSK has never been used in any specifications it can be specified in such manner that it is acceptable to all lower layers. A Usage Specific Root Key (USRK) can be derived from the EMSK and used for efficient re-authentication within the EAP framework. In HOKEY terminology this key is called re-authentication Root Key (rRK). The rRK on its turn is used to derive the re-authentication Integrity Key (rIK) and a re-authentication MSKs (rMSK) that is specific to each authenticator that the MN associates with. The rIK is used to prove being a party to the full EAP method-based authentication and is used in a proof of possession exchange between the MN and the AAA-server. Finally, the rMSK is used for deriving the TSK after each re-authentication phase (see Figure 4).

One of the most important features of the HOKEY key hierarchy is that it doesn't require the MN to interact with the home domain for authentication purposes when roaming within a foreign domain.

Since HOKEY is still work in progress, a number of issues with its usage in 3GPP SAE/LTE haven't been addressed yet. One of them is related to dealing with the heterogeneity of the authentication mechanisms. Different network technologies use different authentication mechanisms. For instance, UMTS networks use the UMTS-AKA authentication mechanism, and EAP-AKA is used in WLANs. Though UMTS AKA and EAP-AKA

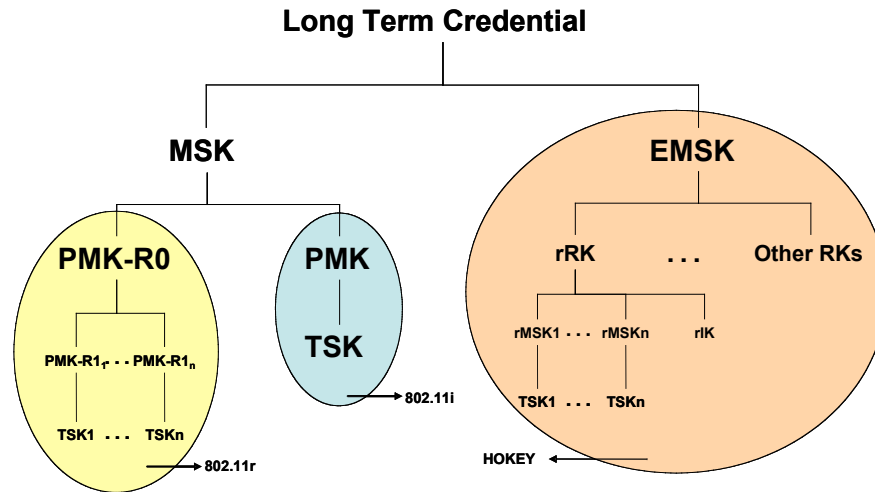


Figure 4: Proposed HOKEY EMSK hierarchy for re-authentication, presented during IETF 66 meeting July 2006.

are almost identical, they differ by the transport method of the AKA protocol: PMM protocol in case of UMTS and EAP protocol in case of WLAN, The former doesn't have a fast re-authentication function, while EAP-AKA [18] does offer such functionality, which makes it better suitable to be used in the EAP-ER framework [19].

Another issue to be solved is the choice of a proper key distribution mechanism. The rMSK must be delivered to the new authenticator following re-authentication. Options for key delivery are either based on a pull or a push model. The push model does not allow randomness contribution by the peer, is not supported by RADIUS, does not scale well, results in keys on target authenticators that the peer may never roam to, target authenticators must store keys, key names, associated nonces, lifetimes, and other attributes for many peers unnecessarily, peer needs to be involved in a re-authentication protocol anyway to receive nonces or other attributes. So there is not much value in the push model. Therefore a peer-initiated, on-demand pull model makes more sense.

For the inter-domain case, key delivery is not straightforward. How does the AAA server know the AP in the foreign domain? How to setup a secure communication channel with the foreign domain? Do the foreign APs communicate with the home rMSK server directly or via their own rMSK server?

IETF PANA [20] is an network access authentication protocol transported over IP, and as such independent of the underlying technology. It

authenticates peers with the EAP protocol, and as such is both an EAP transport and an EAP lower layer, like IEEE 802.1x. The Media Independent Pre-Authentication (MPA) approach [21] tries to define a solution for pre-authentication that support both inter-domain and inter-technology handovers. MPA is a mobile-assisted higher-layer authentication, authorization and handover scheme that is performed prior to establishing link layer connectivity to a network where the MN may move in near future. In MPA, the notion of 802.11i pre-authentication is extended to work at higher layer, with additional mechanisms to securely perform early acquisition of an IP-address from the new network as well as pro-active handover to this network while the MN is still attached to the current network. MPA provides a secure and seamless mobility optimization that works for inter-domain heterogeneous handovers.

6. Analysis

To evaluate the existing solution we consider a number of principles that serve as guidelines in this paper to evaluate handover solutions. These guiding principles can be related to the architecture, performance and security aspects of the solutions. The architectural guidelines considered are reusability (i.e., to be able to use the solution again to add new functionality with minimum modifications) and modularity (i.e., the solution is composed of components with well defined functionality and interfaces). Requiring a handover solution to be fast, we consider the following performance guiding principles for such a solution: support of different air interface technologies (as mobile devices are equipped with multiple network interfaces nowadays), compatibility of local and global mobility solutions (as mobile devices are going to cross over administrative domain boundaries frequently), and support of multiple air interfaces being active simultaneously (when possible and appropriate). The latter requires the solutions to be energy effective. The security related guidelines include binding L2, L3 and higher layers to the user as identified by its USIM.

For our analysis we consider three categories of protocols or (partial) solutions and evaluate them based on our guiding principles mentioned. These solution categories are: mobility/handover solutions, authentication methods, and authentication transport protocols. Mobility or handover management related solutions that we consider are: MIPv6, HMIPv6, FMIPv6, MOBIKE, NetLMM, MPA, IEEE802.21, IEEE802.16/e and IEEE802.11. For authentication methods we investigate UMTS-AKA, EAP-AKA, EAP-TLS, 802.11i, and EAP-ER. Finally, we consider EAP

and combined PANA and IPsec as authentication transport protocols for our analysis. Figure 5 presents a summary of our analysis. One should note that key establishment/distribution aspects that are provisioned in for example IEEE802.11i, IEEE802.11r, IEEE802.16, EAP-ER, HOKEY, IKE and AKA) are already included in one or more categories identified above. A close investigation of the results of Figure 5 reveals that a complete system architecture is missing to deliver secure and fast handover management. Such architecture must provide integrated security management to deal with threats in all handover phases.

<i>State of the art analysis</i>	reuse		modularity		local mobility		global mobility		support multiple air IFs		L2 binding		L3 binding		uses SIM	
	architecture		fast				secure									
Mobility																
MIPv6			~	y	y		n	y								
HMIPv6			y	n	y		n	y								
FMIPv6			y	y	y		n	y								
MOBIKE				y	y		n	y								
NetLMM			y	n	n		n	y								
MPA						y	y	y								
802.21						y										
802.16/e			y	n	y		y	n								
802.11			y	n	y											
Auth & keying																
UMTS-AKA	n	n					y								y	
EAP-AKA						y	y								y	
EAP-TLS						y	y									
802.11i						y	y	n								
EAP-ER																
Auth transport																
EAP						y	y	y								
PANA + IPsec															y	

Figure 5: Comparison of (partial) solutions for supporting mobility in SAE/LTE.

7. Conclusions and Future Work

In this paper we have presented an overview of SAE/LTE and IP layer mobility protocols and key management solutions that can be used for SAE/LTE. Based on analysis that utilizes principles coming from SAE/LTE requirements we come to the conclusion that EAP-ER using AKA is the authentication and key agreement solution that should be utilized for SAE/LTE. The study also shows that NetLMM and MIP are the mobility solutions that can be used. The results to some extent are in contradiction to what is currently accepted in 3GPP.

From network layer protocol perspective 3GPP is focusing on NetLMM and MIP but also has accepted GTP. Obviously the acceptance of GTP is due to the fact that existing solutions can be reused. As for key agreement 3GPP has a working assumption of UMTS-AKA. This working assumption certainly works fine for fast mobility between UMTS and LTE but it does not cater for future where there will be integration of other RANs.

This work still leaves us with the need to study the integration of mobility protocol and key management solution in the SAE/LTE architecture. This integration should be done while considering the security and mobility aspects. Another point to study is the key hierarchy required for SAE/LTE. This can easily be concluded by looking at the end-point of different protocols (MAC, RRC, NAS and U-plane) and the confidentiality/integrity requirement. Once all is done a study on remaining threats and performance is also required.

References

1. 3GPP Gantt Chart, <http://www.3gpp.org/ftp/Specs/html-info/GanttChart-Level-2.htm#32085>
2. 3GPP TR 25.913: "Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN)".
3. 3GPP TR 25.912: "Feasibility Study for Evolved UTRA and UTRAN".
4. 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Overall description; Stage 2".
5. UTRA-UTRAN Long Term Evolution (LTE) and 3GPP System Architecture Evolution (SAE), <http://www.3gpp.org/Highlights/LTE/LTE.htm>.
6. mITF: "Mobile IT Forum 4G Mobile System Requirements Document," Ver. 1.1.

7. 3GPP TR 25.814: "Physical layer aspects for evolved Universal Terrestrial Radio Access (UTRA)".
8. 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolved RAN/3GPP System Architecture Evolution".
9. 3GPP TS 33.922: "Security aspects for inter-access mobility between non 3GPP and 3GPP access network".
10. 3GPP TR 23.401: "General Packet Radio Service (GPRS) enhancements for Long Term Evolution (LTE) access".
11. 3GPP TS 23.402: "3GPP System Architecture Evolution (SAE): Architecture enhancements for non-3GPP accesses".
12. 3GPP TR 22.258: "Service requirements for an All-IP Network (AIPN); Stage 1".
13. 3GPP TR 22.978: "All-IP Network (AIPN) feasibility study".
14. 3GPP TR 23.882: "3GPP System Architecture Evolution: Report on Technical Options and Conclusions".
15. 3GPP TR 21.902: "Evolution of 3GPP system".
16. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
17. IETF Handover Keying (HOKEY) working group <http://www.ietf.org/html.charters/hokey-charter.html>
18. J. Arkko and H. Haverinen, EAP AKA Authentication, Internet Draft draft-arkko-ppext-eap-aka-13, Oct. 2004.
19. V. Narayanan and L. Dondeti, EAP Extensions for Efficient Re-authentication, Internet Draft, draft-vidya-eap-er-02, expires July 23, 2007.
20. IETF Protocol for carrying Authentication for Network Access working group <http://www.ietf.org/html.charters/pana-charter.html>
21. Ashutosh Dutta, Tao Zhang, Yopshihiro Ohba, Kenichi Taniuchi, Henning Schulzrinne, "MPA assisted Optimized Proactive Handoff Scheme," ubiquitous, pp. 155-165, The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005.