Technical Report N°: T2.1_2005_PR_R02

WLAN/3G secure authentication based on SIP

S.Salsano [1], G. Martiniello [2], L. Veltri [3]

I. Introduction

Third-generation (3G) cellular systems will provide global coverage and nearly universal roaming, offering data rates up to 2 Mb/s. The down side is that the deployment and management cost of 3G networks is high. On the other hand, wireless LAN (WLAN) systems are more suited for hotspot coverage and offer data rates that easily exceed 3G data rates with low investment cost. Hence, integrating the two systems would allow operators to take advantage of their best features.

A typical way to consider the integration of 3G with WLAN foresees to give access to resources and services offered by a 3G system using a terminal with a WLAN interface[1]. Given its widespread penetration, most of the existing work in this area has focused on IEEE 802.11 (“Wi-Fi”) as WLAN technology, so that the integration/interworking of 3G with WLAN discussed in [1] is narrowed down to the issue of 3G-WiFi integration. In this paper we try to provide a solution with a broader applicability range and in particular:

we defined an authentication mechanism which is independent respect to the 802.11: the overall architecture applies to UMTS, WiFi, or other access technology;

we implemented and tested our solution on a mobile terminal with UMTS, WiFi, and Bluetooth wireless interfaces.

The paper is structured as follows: in Sections II and III the authentication mechanisms for WLAN and 3G networks are briefly recalled; in Section IV the main issues on 3G-WLAN interworking are discussed; in Section V the proposed solution is presented, while in Section VI our implementation testbed is described. Finally conclusions are drawn in Section VII.

II. Wireless LAN Access: Authentication Mechanisms

A simplified view of a generic wireless access architecture is reported in Figure 1. A mobile terminal (MT) accesses a set of services via a wireless access network. Depending on the context, the services could be offered to every users (“no-authorization” services) possibly restricted a local subset of services, and/or to authorized users (“subscription-based services). In the latter case it is very important to have a robust authentication and authorization procedure in order to grant access to the mobile user.

There are several mechanisms that can be involved and there is not a prevailing standard way to perform it. Some mechanisms are specific to the wireless access technology and they will denoted here as “data link-layer” or “layer-two” (L2) mechanisms. Other authentication mechanisms logically belong to the “network layer” (IP) or to the upper layers (transport or application layer), so that they are independent of the wireless technology.

For IEEE 802.11 WLANs there are defined some L2 access control and security mechanisms specified by IEEE 802.11-1999, IEEE 802.1X, and IEEE 802.11i standards [2]. The authentication framework is based the Extensible Authentication Protocol (EAP) and involves the MT, an intermediate node (the access point) acting as authenticator, and a back-end authentication server (AS).

However, in most of currently offered WiFi “public services”, authentication and authorization are performed at upper layers, placing an authentication gateway/access server between the wireless access and the services. L2 access is not controlled, but MTs are forced to authenticate against the gateway/access server before receiving service grants. Such access mechanisms are often referred as “Captive Portals”. A rather common approach is to adopt a simple web based interfaces to perform the authentication. When a user attempts to browse to any web page, the captive portal will force un-authenticated users to provide some credentials. In order to perform authentication and authorization, the server may use a remote AAA server (for example using RADIUS or Diameter). With this approach the security level is often rather low; in fact there is often only an initial authentication/authorization of the user, but no authentication of the data (neither encryption) is performed.

The wireless access can be also secured by using VPN technologies like the Point-to-Point Tunneling Protocol (PPTP), L2TP (Layer-two Tunneling Protocol) or IPSec. In these cases the authentication of the end systems/users is based on shared secret, private/public keys, or digital certificates.

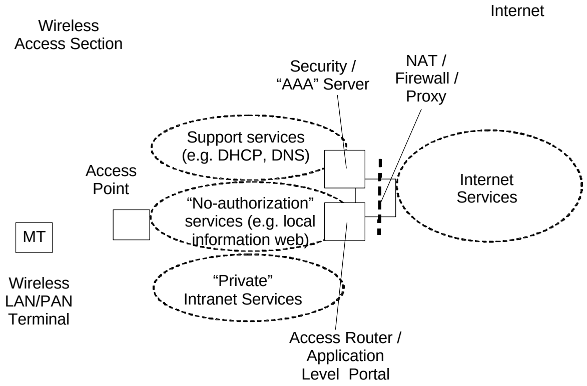
Internet
Wireless Access Section
Security / "AAA" Server
NAT / Firewall / Proxy
Support services (e.g. DHCP, DNS)
Access Point
"No-authorization" services (e.g. local information web)
Internet Services
MT
Wireless LAN/PAN Terminal
"Private" Intranet Services
Access Router / Application Level Portal

Figure 1. Exemplary Wireless LAN/PAN access architecture

III. Authentication in 3G Networks

The authentication architecture of 3G networks is based on two different subscriber's individual secret keys that are stored in two virtually-different subscriber modules called USIM (UMTS SIM) and ISIM (IP multimedia SIM). The two keys K_U and K_I are shared with the Home Subscriber Server (HSS).

The authentication procedure in 3G is called Authentication and Key Agreement (AKA). AKA is a challenge-response mechanism for mutual authentication and session keys generation. AKA is used both for radio network authentication and IP Multimedia Subsystem (IMS) authentication purposes (respectively using K_U and K_I).

The authentication procedure is represented in Figure 2.

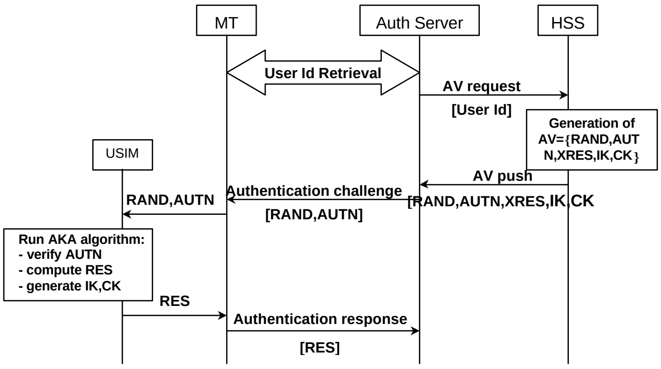

Figure 2. AKA successful procedure

The HSS is responsible for producing authentication vectors (AVs), based on the secret key and on a sequence number SQN. An AV contains: a random challenge RAND, a network-authentication token AUTN, an expected result XRES, a session key for integrity check IK, and a session key for encryption CK. When needed, the AV is passed to the authentication server located in the home network (the S-CSCF in case of IMS authentication) that uses it to create a new authentication request for challenging a new supplicant MT. The authentication request is delivered to the USIM used by the MT that verifies the AUTN, using the secret key K and the sequence number SQN. If AUTN and SQN are valid, the network is authenticated and the USIM can locally calculate the authentication result (RES) and the session keys IK and CK. The RES is then sent to the authentication server for MT authentication. The authentication server compares the RES value with the expected response XRES. If it matches, the MT/user is authenticated and the session key IK and CK can be used to protect further communications between MT and home network. Details on AKA can be found in [3].

A. Authentication in the IP Multimedia Subsystem

The control plane of the IMS [4] is based on SIP (Session Initiation Protocol) [5]. Particularly, Figure 3 shows the authentication framework that involves the following nodes:

- P-CSCF (Proxy – Call Session Control Function), which is the first point of contact for the User Equipment (UE) inside a IMS and can be located in the Visited Network or in the Home Network; it acts mainly as SIP Proxy Server between the UE/MT and the I-CSCF/S-CSCF;
- I-CSCF (Interrogating – Call Session Control Function), which is the main contact point for the MT inside the Home Network; it routes signaling messages towards and from the S-CSCFs but it is an optional IMS element that principally allows to hide the home network topology;

- S-CSCF (Serving – Call Session Control Function), which is the actual SIP Registrar Server for local users, and implements session control functionality and service triggering for all registered users, whether they are in the Home Network or they are roamed in a Visited Network; it interacts directly with the HSS performing authentication procedure;
- SEG (Security Gateway), an entity on the border of the IP security domain, which is used to protect IP communications enforcing security policies over interface between different domains. The security may include filtering policies and firewall functionality;
- HSS (Home Subscriber Server), the master database and stores subscription and location information and profiles.

The S-CSCF communicates with the HSS using the Diameter protocol.

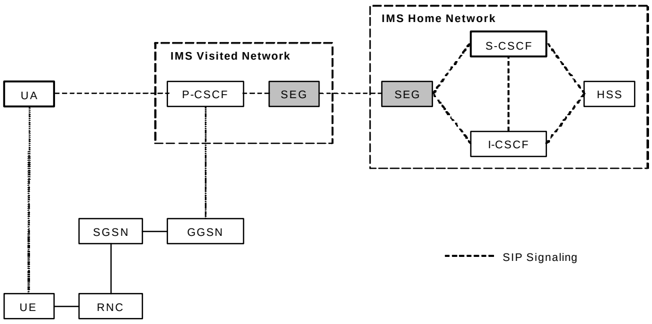

Figure 3. IMS authentication architecture

In order to access to the IMS, a MT should perform complete *GPRS Attach* procedure and establish a PDP (Packet Data Protocol) IPv6 context between the SGSN (Serving GPRS Support Node) and the GGSN (Gateway GPRS Support Node). After the IPv6 tunnel has been created the MT gains IP connectivity and can be configured by the GGSN with the suited P-CSCF in the Visited Network.

Before a user can get access to the IP multimedia services he/she must authenticate with the IMS at application level and at least one IP Multimedia Public Identity (IMPU) (i.e. a SIP or TEL URI) needs to be registered with the suitable S-CSCF of the Home Network. The (mutual) authentication is based on AKA.

However, 3G networks provide independent authentication mechanisms for the PS/CS domains and for the IMS domain. This means that, before accessing to IMS, double authentication is performed (with the PS domain and with the IMS).

This IMS authentication procedure takes place between the MT (actually a SIP User Agent within the MT), and the Home Network S-CSCF, which acts as a SIP Registrar Server and retrieves user profile and AVs from the HSS. During the authentication procedure the MT and the first P-CSCF agree on algorithms and parameters for establishing two pairs of IPSec ESP Security Associations in order to guarantee privacy and integrity for all SIP messages exchanged by the two nodes. In particular the integrity key and the ciphering key are derived from key material obtained with the AKA mechanism.

After successful authentication, the MT is registered and ready to set up or receive calls using SIP. It is responsibility of MT to refresh the registration before it expires and each registration procedure requires a new authentication vector.

IV. Authentication Issues in WLAN-3G interworking

The fundamental requirement set by the 3GPP for 3G-WLAN interworking is that the UMTS security architecture (defined in [3]) must not be compromised. The 3GPP specifies that the authentication scheme between a WLAN terminal and its 3G home network must be mutual and based on a challenge-response mechanism, and all long-term security credentials used for subscriber and network authentication must be stored on a smart card like tamper resistant device. Moreover the selected authentication scheme must support agreement of session keys. All these requirements lead to the adoption of UMTS AKA procedure and to the re-use of 3GPP subscription system. Thus WLAN terminals should need to access to UICC (UMTS Integrated Circuit Card) smart cards with USIM/ISIM applications.

In the intention of the 3GPP, 3G-WLAN interworking should also take advantage of the link layer security provided by WLAN technologies. However the requirements are not completely defined. A detailed analysis of authentication issues in 3G-WLAN interworking can be found in [8] and [9].

V. Proposed approach for WLAN-3G authentication

In this section a generic open solution for secure authentication in a 3GPP–WLAN interworking scenario is proposed. The proposal addresses the generic scenario in which an user needs to be authenticated in a WLAN or PAN access network using the credential in his/her 3G SIM. This authentication could be in principle independent from a “traditional” registration in the 3G IMS: for example the user could have his/her 3G mobile phone switched on and registered to the CS/PS/IMS 3G domains, and in parallel have his/her laptop accessing a WLAN hotspot using 3G credentials. In [10] the authors analyze this last scenario considering the interaction between a laptop and a 2G SIM. Another example could be that of a PDA with dual WLAN/3G interfaces being registered on the 3G interface for receiving multimedia calls and accessing Internet via the WLAN interface.

The proposed authentication procedure is based on registration functionalities and authentication features offered by Session Initiation Protocol (SIP) [5], and it is performed with the mechanism used by IMS. However, while the authentication defined for IMS in 3GPP somehow “complements” an authentication performed at lower layer, we propose to operate directly this SIP based authentication, using it also for gaining initial access to a Wireless LAN/PAN. The authentication mechanism defined in IMS is now considered as a common authentication framework applicable also to non-3G services as those provided directly by the non-3G wireless access network (e.g. for Internet access managed by the hotspot operator).

According to the 3GPP model described in section IV, a MT gaining access through a WLAN based system should first perform a L2 procedure (EAP-AKA) procedure to authenticate with access network, and then perform SIP-Digest-AKA procedure in order to authenticate with the IMS and access to IMS services. This model has the following drawbacks: i) two authentication procedures are required, ii) the WLAN system must implement complete layer-two authentication and authorization mechanism (the EAP-AKA).

The basic idea is to move the authentication functionality from layer-two (802.1x/ EAP-AKA) to the service level (SIP-Digest-AKA), enforcing also confidentiality and access control directly at IP layer through IPSec and packet filtering functions. This has a twofold direct benefit: on the one hand only one authentication between the MT/UA and the access network is now required, speeding up authentication and roaming latency, on the other hand moving the authentication functionality to upper layer considerably increases access and configuration flexibility. Using IPSec as common security platform (together with SIP-Digest-AKA authentication) has the advantage to make the roaming procedure completely independent from the specific access technology (layers one and two). The same procedure for example may apply in case of IEEE 802.11 WLAN, Bluetooth, or other new incoming technologies. Moreover the IPSec encapsulation and security mechanisms easily allow the extension to new encryption algorithms and the selection by the mobile operator of the most suitable, without changing the access network hardware infrastructure. The only potential disadvantage of such approach may consist on the increase of processing capability required on the access router (i.e. the SEG) implementing IPSec. However, such increase can be overcome by the new processing capability of current high-speed router CPUs and by the hardware implementation of routing and security functions (e.g. by using harware accelerator cards).

Figure 4 shows the architecture of the proposed solution. The innovation with respect to the “traditional” 3GPP approach is the introduction of SIP functionality in the access network. Since the MT authentication is now based on SIP Digest/Digest AKA, the access network should provide SIP/IP connectivity through interfaces Ww and Wa, and P-CSCF functionality, while the MT should natively support SIP UA functionality. The confidentiality and integrity protection of SIP signaling and data over the interface Ww is provided using IPSec while the protection of SIP signaling over the interface Wa (i.e. between WLAN P-CSCF and IMS P-CSCF) can be provided using any standard way to protect SIP inter-proxy communication (e.g. IPSec or TLS). The IPSec security associations (IPSec SAs) between the MT and the access network P-CSCF are dynamically negotiated and established during the authentication procedure through the security agreement functionality provided by SIP [11]. After the authentication procedure has been successfully completed, SIP security agreement functionality is further used to negotiate a second IPSec SA between the MT and WLAN SEG for protecting the UA data exchanged through the air interface. Access control is performed on the access network by the SEG node (the access router) through packet filtering. Only users correctly authenticated with the access network are enabled by the SEG to gain IP connectivity with the 3G (visited) network (through interface Wn) and/or to an external IP network (intranet/Internet) directly by the access network SEG/AR. All the traffic of unauthorized users is filtered by the SEG, and unauthorized UAs are allowed to communicate only with the P-CSCF (in order to perform authentication).

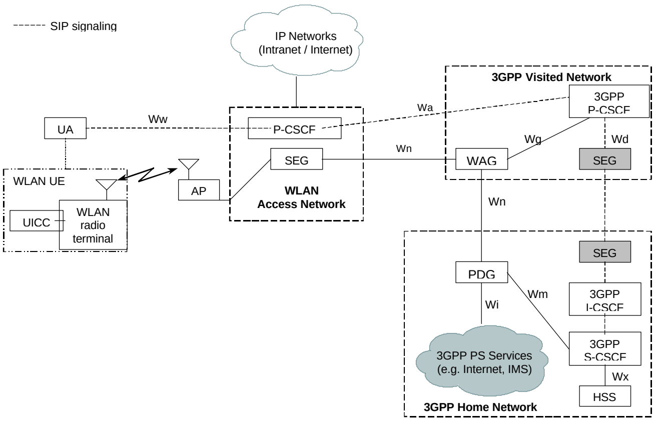

Figure 4. Proposed authentication solution architecture

A. *Proposed authentication procedure*

In this section, we describe the proposed authentication procedure. Further details, including for example the analysis of unsuccessful procedures, can be found in [12]. When the MT roams onto a new network, first it tries to associate with a wireless Access Point (AP). This could be done with or without layer-two security support depending on the specific implementation; anyway the further communication will be completely secured at upper layer with IPSec, and layer-two security is not necessary. After the association with the AP the MT dynamically configures its IP layer by means of DHCP function implemented in the access network. The DHCP server may provide to the MT together with basic IP configurations under service related configuration such as a default outbound proxy (i.e. the P-CSCF).

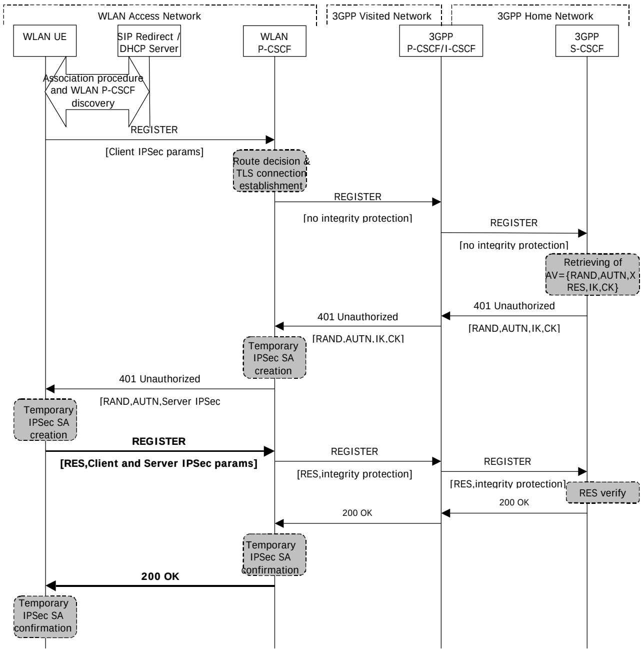

Figure 5. Successful authentication procedure

The authentication procedure starts with a SIP REGISTER request sent by the UA to its home network. The address of the I-CSCF is obtained by resolving the home network domain name, that is stored within the UICC smart cards containing both the USIM and ISIM applications. This REGISTER message may indicate the type of service is required, for example it could indicate that only a WLAN access is requested and not a "traditional" IMS registration. The mechanism used to specify such information is described in the next subsection B.

Since in this initial phase the MT is still filtered by the access router/SEG, the SIP REGISTER request is sent through the access network P-CSCF. There are several mechanism that can be used by the MT to obtain the address of the access network P-CSCF: 1) via the specific DHCP configuration SIP server option; 2) resolving the visited network domain name via DNS; 3) via SIP redirect functionality responding at the default SIP port 5060 of the WLAN default gateway (a SIP redirect server may respond to the MT with a SIP 305 "Use Proxy" redirection response indicating the IP address of the real WLAN P-CSCF).

Within the REGISTER request message the MT sends various information required for the registration and authentication procedure to the WLAN P-CSCF and to the its home 3G S-CSCF, such as the value of the private user identity, the public user identity to be registered, the IP address and port of the MT, and the duration of the registration. Moreover, by means of the SIP security mechanism agreement [11], the MT specifies the IPsec layer algorithms and protocols supported as well as the parameters needed for the SA setup by the WLAN P-CSCF.

Upon receiving the SIP REGISTER request, the WLAN P-CSCF indicates in the SIP authorization header field that the request was not received integrity protected with a SA. Moreover, according to SIP security mechanism agreement, P-CSCF checks, removes, and stores information about IPsec layer algorithms and parameters needed for the SA setup. Then the WLAN P-CSCF determines the next hop and forwards the request (establishing an opportune TLS connection to this node if needed). If the wireless access network is federated or belongs to a foreign 3G network the next hop will be a 3GPP visited network P-CSCF while if the wireless access network belongs to or is federated to the user's home 3G network, the next hop will be a 3GPP home network I-CSCF or directly the 3GPP home network S-CSCF.

The request is then routed via 3GPP P-CSCF/I-CSCF to the 3GPP S-CSCF as defined for IMS. Upon receiving the SIP REGISTER the 3GPP S-CSCF identifies the user by the user identity and uses an Authentication Vector (AV) to challenge the MT by generating a 401 "Unauthorized" SIP response, which contains the RAND and AUTN AKA parameters, the integrity key IK and the ciphering key CK.

This challenge is delivered back toward the MT via the reverse SIP route. When the WLAN P-CSCF receives the message, it removes the CK and IK values and binds them to the proper private user identity. It then selects the parameters needed for the SA setup by the MT, sets up a temporary set of IPSec SAs using the parameters and algorithm values associated with the private user identity and sends the response to the MT using the new SAs.

Upon receiving the challenge the MT checks the RAND and AUTN AKA parameters. If the check is successful the MT calculates the response (RES parameter) and derives the keys CK and IK. Then it sets up a temporary set of SAs based on the algorithm and parameters (specified in the response by WLAN P-CSCF) and on its capabilities sent in the original REGISTER request and sends another REGISTER request protected with the temporary set of SAs. In addition to the header fields already present in the initial request, the MT includes the computed authentication challenge response RES. According to the SIP security mechanism agreement the MT inserts the same IPsec layer algorithms and parameters already included in the previous REGISTER request and it mirrors those specified by the WLAN P-CSCF in the received response.

Upon receiving the new SIP REGISTER request, the WLAN P-CSCF indicates in the SIP *authorization header* that the request was received through a protected connection (with a SA either created during an ongoing authentication procedure or during the last successful authentication procedure). Upon receiving new integrity protected REGISTER request, the S-CSCF checks the response sent by the MT. If the check is successful then the user has been authenticated. The S-CSCF then sends back a 200 "OK" SIP response to the MT.

When the WLAN P-CSCF receives the 200 "OK" response, it changes the temporary set of SAs (SAs) establishing new SAs. Then the WLAN P-CSCF instructs the access router/SEG to modifies its firewall rules in order to enable network connectivity to the authenticated MT, and forwards the response to the UA (protected within the SA). On receiving the "200 OK" response, the MT changes the temporary set of SAs and use the newly established set for exchanging messages with the SEG/WLAN P-CSCF. Further details on the establishment of IPSec Security Association can be found in [12]. Port values for all the SAs are communicated to the peer SIP agent using SIP security mechanism agreement [11]

At this point, the MT is authenticated in the new access network and can be authorized to access all services that it is enabled to. If the initial REGISTER message indicated that only a WLAN access was requested and not a "traditional" IMS registration (as we assumed earlier in this section) the MT will not be registered in the IMS for 3G multimedia services. Of course it is also possible that the MT wants to register to the IMS in a "classical" way from its WLAN access, in this case a single registration procedure will authenticate the MT, authorize it to access the network and register it in the IMS as needed to receive multimedia 3G services.

B. SIP extension for WLAN services indication

The SIP Registration procedure has been used as generic authentication method for a MT equipped with a valid 3G SIM that roams into an access WLAN. According to the proper roaming model, the MT may or may not want access to 3GPP services on the visited/home networks via the WLAN. In order to simplify the proper service class selection (3GPP home, visited, none, etc.), a common solution should be used. In this section a simple mechanism is proposed for letting the MT indicate to its S-CSCF which services it is willing to use on the new attachment point. The proposed mechanism makes use of the SIP extension defined within the IETF to let an user agent to convey its capabilities and characteristics to other user agents and servers. Such information is conveyed as parameters of the *Contact* header field, as in the following example:

```
Contact: <sip:alice@host.domain.net>;audio;video
           ;mobility="fixed";methods="INVITE,BYE,OPTIONS,ACK,CANCEL"
```

We extends such mechanism by defining the new parameter "*3gpp-services*" indicating which services the MT is able/wants to access through the new registered contact address (corresponding to the new point of attachment). For example, by filling the *Contact* header filed of the REGISTER message in the following way:

```
Contact: <sip:alice@host.visited-hotspot.net>;mobility="mobile";3gpp-services="all"
```

the UA indicates to the S-CSCF that it is able to access to all services the UA is allowed/authorized to.
The value of the parameter *3gpp-services* together with the *qvalue* (if present), have to be intended as an hint for the S-CSCF that will decide the actual URI service profile taking also into account other information such as the user profile, some pre-configured options, the service roaming agreement between home and visited network.
The value of the *3gpp-services* parameter is completely implementation dependent. The only two values that are here defined are “all” (no limitation) and “none” (no 3GPP services available). For example, an UA that fills the following Contact header within its the REGISTER message

```
Contact: <sip:alice@200.100.5.33>;mobility="mobile";3gpp-services="none"
```

indicates that the new URI `sip:alice@host.domain.net` has to intended just as the a new point of attachment identifier and not as a 3GPP-capable URI. This, for example, may apply in case the MT is within a hotspot the is using the SIP Register capability (as discussed earlier in this paper) only for authentication purpose, and not for accessing to 3GPP services.
In general, the MT may fill the *3gpp-services* parameter based on mechanisms like:

- a pre-configured roaming behavior, eventually dependent on the type of devices (e.g. phone, PDA, or laptop), or on the identity of the visited domain,
- an explicit hint by the user,
- by interrogating (through other mechanisms) the visited network about the supported services and the roaming agreements with the home network.

Regarding the third mechanism, the UA might query the WLAN P-CSCF for local capabilities by sending an OPTIONS request message. For example, a WLAN P-CSCF that acts only as authenticator and not as entry point to 3GPP services, could respond to an OPTIONS message

```
OPTIONS sip:proxy.visited-hotspot.net SIP/2.0

```

...
by sending the following response:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pc33.visited-hotspot.net;branch=z9hG4bKhjhs8ass877
To: <sip:proxy.visited-hotspot.net>;tag=93810874
From: Alice <sip:alice@alice-provider.net>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 63104 OPTIONS
Allow: REGISTER, OPTIONS
Content-Length: 0
```

indicating that only REGISTER and OPTIONS methods are allowed (no invited sessions allowed).

VI. IMPLEMENTATION TESTBED

The proposed architecture has been implemented in a testbed comprising both registration and security aspects. In the testbed, a MT (a laptop PC) can access indifferently to 3G/UMTS network via a connect card, to a IEEE 802.11 WLAN, or to a Bluetooth access link. The UMTS is used only as WAN access technology, and CSCF nodes and HSS have been locally re-implemented in the testbed.
The support for the core Bluetooth layers and protocols has been provided using BlueZ [12], the Linux Bluetooth protocol stack, details on using Bluetooth stack for IP access can be found in [18]. The two local wireless access networks and the wired network are interconnected through an access router implemented with a Linux box that hosts also a SIP Proxy (the WLAN P-CSCF) and packet filtering functionality (through Linux netfilter/iptables). The wired network interconnects the AR, a SIP Proxy/Registrar (the S-CSCF) running on a Linux box, and the public Internet. The MT is equipped with the three wireless interfaces and hosts a specifically deployed SIP UA which only includes registration and authentication functionalities. The SIP applications (servers and user agents), implemented in Java, support standard 3GPP/IMS SIP signalling and have been developed starting from the implementation described in [14] and using MjSip as open source SIP stack [15]. In particular, the mobile UA and the two servers have been extended in order to support SIP AKA registration as described in the previous sections. The mobile SIP UA, which performs the registration and authentication on behalf of the user, communicates with the UICC smart card via the (serial) smart card reader GemPC410, manufactured by Gemplus [16]. This communication is enabled by the OpenCard Framework (OCF) [17] and allows the SIP UA to request to the SIM/USIM application the execution of the cryptographic algorithms needed to perform authentication. OCF provides high level Java APIs whose purpose is to make the functionality and the information contained in the UICC fully accessible hiding the complexity of interacting with the smart card. Finally, IPSec functionality has been activated in both the MT and the AR/SEG (that is also the WLAN P-CSCF) on the WLAN and Bluetooth interfaces. Figure 6 shows the overall testbed layout.

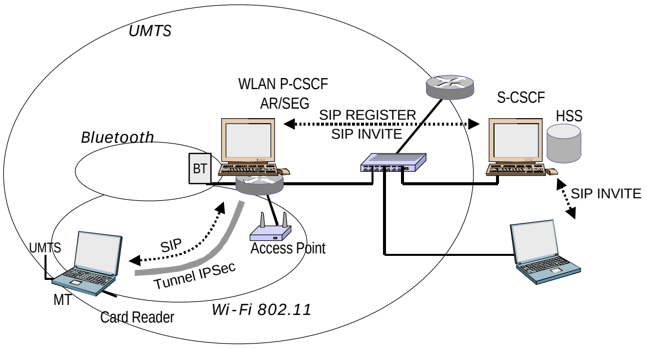

Figure 6. Implementation testbed layout

In our testbed we simulated the 3G USIM used for AKA functionality through a standard 2G SIM, accommodated in the UA, since the 3G SIM would require the knowledge of authentication credential in the real HSS.
Figure 7 shows the implementation architecture of the UA, P-CSCF/SEG, and S-CSCF. The entire service layer (SIP UA and P/S-CSCF systems) has been implemented in Java, while the network layer has been based on open source products (FreeSWan for IPSec and Linux netfilter for the SEG packet filter).

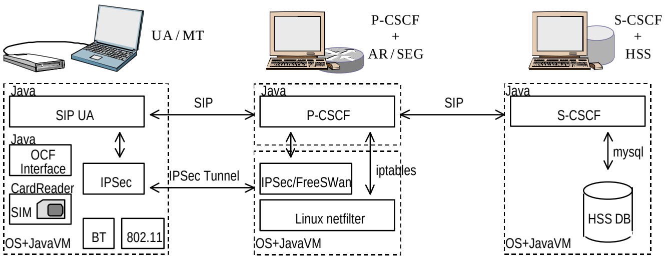

Figure 7. Implementation architecture

VII. References

[1] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) Interworking; System Description".

[2] IEEE 802.11i, " Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements", June 2004.

[3] 3GPP TS 33.102: "Security architecture".

[4] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)".

[5] J. Rosenberg et al., "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[6] S. Salsano, L. Veltri, and D. Papalilo, "SIP Security Issues: The SIP Authentication Procedure and its Processing Load", IEEE Network, November/December 2002.

[7] A. Niemi, J. Arkko and V. Torvinen, "HTTP Digest Authentication Using AKA", RFC 3310, September 2002

[8] K. Ahmavaara, H. Haverinen, R. Pichna, "Interworking Architecture between 3GPP and WLAN Systems", IEEE Communications Magazine, November 2003.

[9] G. M. Køien and T.Haslestad "Security Aspects of 3G-WLAN Interworking", IEEE Communications Magazine, November 2003.

[10] A. Ahmad, R. Chandler, A. Dharmadhikari, U. Sengupta, "SIM-Based WLAN Authentication for Open Platforms", Technologhy @ Intel Magazine, Intel Corporation, August 2003

[11] J. Arkko et al., "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", RFC 3329, January 2003.

[12] G. Martiniello, S. Salsano, L.Veltri, "Technical Report – Procedures for unified authentication in Wireless LAN/PAN using 3G credentials", http://www.tlc.unipr.it/veltri/wlan-3gpp-interworking

[13] BlueZ, Official Linux Bluetooth protocol stack, http://www.bluez.org/

[14] S. Salsano, L. Veltri, "QoS Control by means of COPS to Support SIP based Applications", IEEE Network, Vol.16 No.2, March/April 2002, pp27-33

[15] MiSip, GPL Java implementation of SIP, http://www.mjsip.org

[16] http://www.gemplus.com

[17] OpenCard Framework (OCF), http://www.opencard.org/

[18] A. Detti, I. Febi, P. Loreti, P. Sperandio, "Bluetooth Handover and Connection Re-establishment in PAN profile", section 2.1.4 of WP4 Vicom Project Deliverable, http://www.vicom-project.it/