# Security Aspects of 3G-WLAN Interworking

*Geir M. Køien and Thomas Haslestad, Telenor R&D, Norway*

## ABSTRACT

Third-generation cellular systems will provide wide coverage and nearly universal roaming, but will not realistically live up to the bit rate expectations placed on them. On the other hand, WLAN systems already offer bit rates surpassing those of 3G systems, but are often found lacking with respect to roaming and mobility support. In short, WLAN systems are great for hot spot coverage, while 3G systems provide global coverage and the necessary network and management infrastructure to cater for security, roaming, and charging requirements. The focus of this article is on security aspects of 3GPP-WLAN interworking.

## INTRODUCTION

Mobile systems like Global System for Mobile Communications/General Packet Radio Service (GSM/GPRS) are immensely successful. The flexibility associated with cellular telephony has gone from being a luxury to becoming a commodity. The present 2.5G systems like GSM/GPRS are capable of delivering IP services, but current cellular systems are still mostly used for speech services. Low bandwidth and expensive data services are perceived to be the main culprits.

Third-generation (3G) systems will improve data capacity and offer data rates up to 2 Mb/s and above, but it is unlikely that the user will be offered the full theoretical capacity since deployment cost is high. This is in contrast to the wireless LANs (WLANs), which provide affordable services and bit rates that easily exceed 3G bit rates. A failing in the current WLAN standard is the lack of sufficient security measures and architecture beyond basic radio access.

Ideally, we would want the subscription management, roaming, and security facilities of a 3G system and the hot spot capacity and low investment cost of WLAN systems. Integration of the two systems therefore aims to combine them such that their best features are kept intact and their weaknesses mediated by the companion system. An important challenge is to reconcile and consolidate the security architectures of the systems.

## BACKGROUND ON 3G-WLAN INTERWORKING

### WIRELESS LOCAL AREA NETWORKS

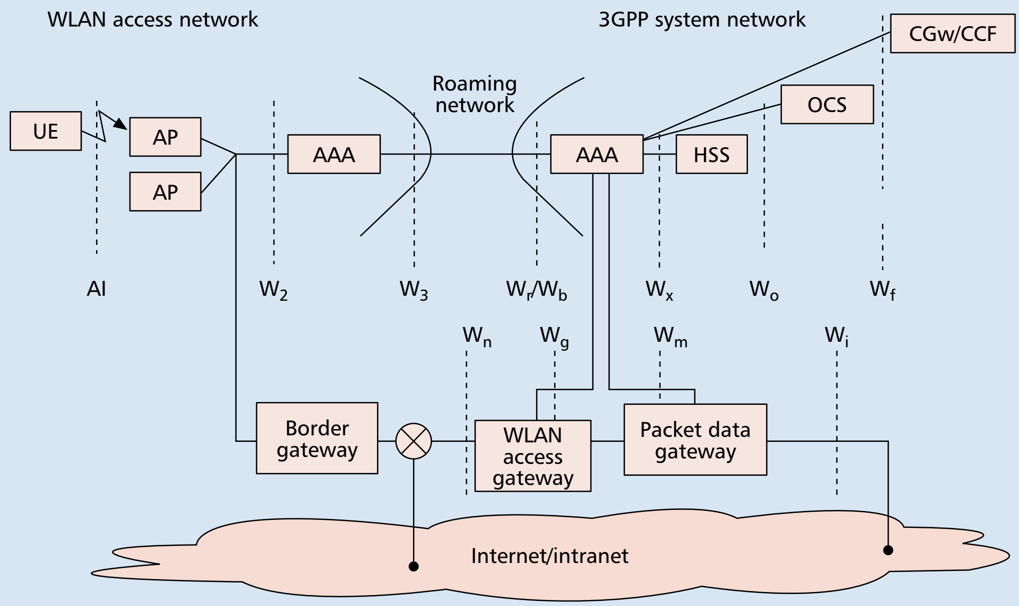
WLAN is, in all simplicity, a cable replacement technology. It provides typical user equipment such as a personal computer with means to move freely within the borders of coverage while maintaining connectivity to the computer's local area network.

IEEE Project 802.11 has provided us with the current WLAN market winning 802.11b standard. 802.11b is the standard for 2.4 GHz and provides bit rates up to 11 Mb/s on the physical medium [1]. IEEE 802.11 also has the 802.11a standard for the 5 GHz band (UNII-band) that provides bit rates up to 54 Mb/s [2]. Please refer to [3] for useful overview of IEEE 802.11 WLAN technology.

ETSI Project Broadband Radio Access Network (BRAN) has published the HIPERLAN/2 [4] standard. This standard provides a WLAN system for the 5 GHz band with integrated quality of service (QoS), security, and bit rates up to 54 Mb/s. Another flavor of WLAN, HiSWANa, also exists. MMAC HSWA is the Japanese organization behind the specification of HiSWANa. HiSWANa is a WLAN system for the 5 GHz band, with capabilities and design that resemble those of HIPERLAN/2. The WLAN community has formed a joint group called WLAN Interworking Group (WIG) [5] in order to be unified on the issues of interworking.

Security-wise the three systems differ. The current IEEE 802.11b deploys confidentiality and integrity protection through a scheme called Wired Equivalency Privacy (WEP). WEP suffers from manual key management and is also cryptographically broken. HIPERLAN/2 and HiSWAN have more advanced confidentiality

0163-6804/03/$17.00 © 2003 IEEE



AI: Air interface as defined within [1–3]
$W_2$: Defines the interface between the WLAN functions and the interworking functions [5]
$W_3$: Defines the interface between the interworking functions and the external network [5]
$W_r/W_b$: The reference point connects the WLAN Access Network to the 3GPP network [7]
$W_x$: This reference point provides communication between AAA infrastructure and HSS [7]
$W_n$: For further study within 3GPP [7]
$W_g$: An AAA interface between the 3GPP AAA proxy and the WAG. For provisioning of information related to the routing enforecement functions for authorized users [7]
$W_o$: This is used by a 3GPP AAA server to communicate with the online charging system (OCS) for charging related information [7]
$W_f$: Provides communication between 3GPP AAA server and charging gateway function (CGF)/charging collection function (CCF) for charging information [7]
$W_i$: Reference point between the packet data gateway and a packet data network (external public or private)

**Figure 1.** *Summary of the proposed architectures for the 3GPP-WLAN interworking.*

and encryption mechanisms. A new enhanced security standard is being specified for IEEE 802.11 that aims to provide enhanced and manageable access security [6].

## The 3GPP System

The Third Generation Partnership Project (3GPP) is a global specification organization for telecommunication and comprises the following organizational partners: ARIB, CWTS, ETSI, T1, TTA, and TTC. Its original mandate was to produce a global specification for a 3G mobile system within the framework set by the International Telecommunication Union (ITU) called International Mobile Telecommunications 2000 (IMT-2000). The cellular system being specified within 3GPP, known as the Universal Mobile Telecommunications System (UMTS), has a new radio system and access network, extensive support for packet data and IP multimedia, and provides a host of other higher-layer services.

Cellular systems such as UMTS and GSM have excellent characteristics in terms of coverage and roaming. Roaming is one of the key factors when identifying reasons for GSM's success. The roaming network and its associated functionality, as we know it today from GSM and GPRS, will exist in the 3G system in a manner that will allow the user to move freely in most GSM/GPRS and UMTS networks.

## Interworking Solution

In ETSI Project BRAN the need for interworking with 3G systems was foreseen early on [7]. The work in ETSI BRAN resulted in two fundamentally different solutions regarding the level of interworking. The two solutions were termed *tight* and *loose interworking* according to the level of integration required between the systems. The tight interworking solution was based on the idea of making use of the WLAN radio interface as a bearer for UMTS with all network control entities in the core network integrated.

*The work in ETSI BRAN resulted in two fundamentally different solutions regarding the level of interworking. The two solutions were termed tight and loose interworking according to the level of integration required between the systems.*

On the other hand, for loose interworking there was little need to make changes to the WLAN standard. This solution has the benefit of not needing a convergence layer, which is an important factor in development time and so on. Loose interworking was therefore adopted as the preferred solution in both the WLAN and 3GPP communities.

With respect to security there are large differences between tight and loose interworking. A tight interworking solution would mandate the full 3GPP security architecture and require the 3GPP protocol stacks and interfaces to be present in the WLAN system. The loose interworking options merely require the 3GPP

*The UMTS AKA procedure relies on the availability of a tamper resistant smartcard at the terminal. The smartcard, called a UICC in UMTS, will run an application called USIM. It is the USIM application that runs the cryptographic algorithms during the execution of the UMTS AKA.*

authentication method to be implemented. To avoid link layer modifications, the authentication protocol is allowed to run at the link layer using Internet protocols — Extensible Authentication Protocol (EAP) and authentication, authorization, and accounting (AAA) — as transport mechanisms.

The main 3GPP-WLAN interworking architecture is defined in 3GPP TS 23.234 [8]; the security architecture is found in 3GPP TS 33.234 [9]. Figure 1 gives an overview of the 3GPP-WLAN architecture.

## Security Concerns in 3G-WLAN Interworking

### Basic Requirements and Assumptions

A fundamental requirement in 3GPP has been that 3GPP-WLAN interworking shall not compromise the UMTS security architecture. Therefore, it is required that the authentication and key distribution be based on the UMTS authentication and key agreement (AKA) procedure.

The UMTS AKA *challenge-response* procedure is largely network-independent, and it is possible to run the AKA procedure over other transport mechanisms. Of particular interest here is the Internet Engineering Task Force's (IETF's) EAP framework [10]. The IEEE 802.11 WLAN already supports EAP through the EAP-over-LAN [11] specification.

3GPP does not assume any specific type of WLAN system, but for the purpose of this article we assume that the WLAN is type 802.11. We note that interworking with other WLAN systems, including the European HIPERLAN/2 and the Japanese HiSWANa, mainly depends on the ability to run EAP methods and to support an AAA interface.

In the 3GPP-WLAN architecture the home network will always be the home environment of the 3GPP system. The requirement on the serving network is for it to support the EAP-AKA authentication method. This implies support for an AAA node that can handle transport of EAP.

The UMTS AKA procedure relies on the availability of a tamper-resistant smartcard at the terminal. The smartcard, called a UICC, in UMTS, will run an application called USIM. It is the USIM application that runs the cryptographic algorithms during the execution of the UMTS AKA. This is an important point since it requires the WLAN mobile station (MS) to be able to access a UICC/USIM. This does not imply that the MS must itself contain a smartcard reader, since it could get access via its host system. We note that this access must be protected.

In order to execute the UMTS AKA procedures over EAP, we needs to define a separate EAP method.[1] The EAP-AKA [12] Internet draft provides exactly this functionality. Note that a similar EAP method exists for GSM/GPRS authentication (EAP-SIM). This EAP method is the basis for 3GPP-WLAN legacy interworking with GSM-only capable smartcards. It will not be discussed further in this article.

### Overview of the Entities and Domains

The following domains and entities are of interest when examining the 3GPP-WLAN security architecture. More information is found in TS 33.234 [9].

***Home Environment (HE)*** — The central network elements in the HE when considering the 3GPP-WLAN architecture is:

- Home subscriber server (HSS): The HSS is the entity containing authentication and subscription data required for the 3GPP subscriber to access service.
- 3GPP AAA server: The 3GPP AAA server is the entity that executes the AKA procedure toward the WLAN subscriber entity (UICC/USIM). The authentication information is retrieved from the HSS.

***Serving Network (SN)*** — In the 3GPP-WLAN context the SN will be the network responsible for the WLAN domain. The WLAN SN may or may not be operated by the HE operator.

- 3GPP AAA proxy: A 3GPP AAA proxy has logical proxying functionality and may reside in any network between the WLAN and the 3GPP AAA server.
- Network access server (NAS): The NAS will be the controller of a set of access points.
- Access point (AP): The APs are the WLAN base stations. They will terminate the radio connection with the mobile station (MS).

***User Equipment*** — The user equipment consists of several entities. Note that the *computing device* may well have an internal WLAN card (MS), so the units may be inseparable.

- UICC/USIM (smart card): The UICC/USIM is the entity that terminates the UMTS AKA sequence. It is presumed to be tamper-resistant. The UICC/USIM is normally owned by the HE operator.
- MS: The MS is the hardware responsible for radio termination (layers 1 and 2). The MS is assumed to be owned and controlled by some non-network operator entity. The entity will terminate the EAP-AKA protocol and request the USIM to do the AKA processing.
- Computing device: The computing device is the entity on which the IP stack is located. Typically this is a laptop PC or PDA. The computing device is assumed to be controlled by the user and owned by the user or some other non-operator organization/entity. No assumption regarding the system integrity of this device can be made.

### Trust Issues

In order to assess and evaluate the possible solutions for 3GPP-WLAN security it is necessary to have a clear picture of the threats the 3GPP-WLAN architecture will face. To address this issue we need to take a closer look at the proposed architecture (Fig. 4). The following questions aim to make the picture clearer:

**Which entities do we trust?** A trust model is needed. Such a trust model would be based on entity ownership control and legally binding con-

[1] *In EAP terminology the support for a specific authentication method is called an EAP method.*

tractual agreements such as the roaming agreements between the mobile operators.

**On what basis do we trust these domains/entities?** The world is not black and white, and one needs to find a balance between risk and opportunity. So on what do we base our trust? Is the foundation solid, or tentative and loose?

**What type of security features are needed to "enforce" the trust?** Without sufficient protection mechanisms our trust could easily be betrayed, by both our "trusted" partners as well as adversaries falsifying and misusing data.

**What would be the goal of an adversary?** Is the adversary content with eavesdropping, or would she also want to engage in active attacks? How resourceful is the adversary? Do we foresee targeted and determined attacks, or do we merely want to offset opportunistic attackers. Can the attacks be automated, or would they be unique events?

A threat analysis is found in TS 33.234 [9]. We also have to consider the nature and basis of the trust relationships. The following provides a brief description. Assumed trust relationships:

**User ↔ HE**: The user and HE will have sufficient trust in each other that the HE is trusted to provide network access, and the user is trusted to pay for attained services. The trust is (often) captured in a legally binding contract that normally has a defined credit limit.

**HE ↔ UICC/USIM**: The UICC/USIM is normally the property of the HE operator. We shall therefore assert that the HE and UICC/USIM can trust each other. However, the HE may cancel and replace the UICC/USIM at any time. The opposite is not true.

**HE ↔ SN**: The trust relationship between the HE and the SN is governed by a legally binding *roaming agreement*. We shall assume that the trust is mutual.

**SN ↔ WLAN access network**: The exact nature of the trust relationship between the SN and the WLAN access network may vary. We assume that there is a binding agreement on service provisioning and charging issues between them.

**User ↔ user equipment**: We shall generally assume that user equipment is controlled by the user. One cannot assume that the user is capable of maintaining the integrity of user equipment. That is, user equipment *cannot* be trusted with respect to security functionality.

## User Identity Privacy

Privacy has many aspects; one of them is location privacy. Location privacy is problematic since there is often a strong connection between the logical identity of the user and the routable address associated with the user device. The primary problem with many access networks is that the link layer (medium access control, MAC) address is visible to anyone by listening to the over-the-air signals. The association between the MAC address and the higher layer user identity is at times also visible or can be forced to be visible. The resourceful adversary could then be able to determine the position of a user with relatively high precision. To mitigate this problem, one often turns to protected temporary identities.

## Lawful Interception

Lawful interception functionality is a mandatory requirement for most 3G operators. There is no reason to expect the 3GPP-WLAN interworking architecture to be exempt from lawful interception requirements. We note that in a roaming environment the access network and core network may be located in different countries and subject to different legislations.

## Authentication, Confidentiality, and Integrity

Given that we have mandated that the 3GPP-WLAN architecture shall use the UMTS AKA procedure, the issue of authentication and key distribution is already taken care of.[2]

Confidentiality is a security service to offer protection against inappropriate disclosure of user or system data. Confidentiality is targeted at protecting the system and user data against passive attacks. 3GPP-WLAN confidentiality services are provided by symmetric key encryption.

The companion security service *integrity* is to provide protection against illicit data modification. Cryptographic integrity protection is thus a security service aimed at protecting data against active attacks. The 3GPP-WLAN integrity service is implemented by (symmetric) keyed cryptographic checksum functions. These functions are known as message authentication codes (MAC); as the name implies, they also provide per message authentication.

It is presumed that the access network can support both confidentiality and integrity services for the over-the-air link. For the IEEE WLAN standard this is problematic in that the current standard only supports the relatively weak and cumbersome WEP method. The forthcoming IEEE 802.11i specification [6] promises to solve this problem. While waiting for the standard to be completed, an interim solution called Wi-Fi protected access (WPA) has been standardized by the Wi-Fi alliance. The WPA method is directly based on the Temporal Key Integrity Protocol (TKIP) of the IEEE 802.11i standard (based on the draft 3.0 version).

Another essential question with regard to the confidentiality and integrity services is how deep into the network the services should extend. For a public WLAN system this is an important question. The access points are small and inexpensive devices. The access points will certainly not be unprotected, but one cannot realistically expect them to offer much in terms of physical protection. Being distributed, one must assume that an adversary will be able to gain physical access to the devices. Then it is naïve to assume that the access points would be able to withstand dedicated attacks. So we face a situation were the APs may not always be able to protect the session keys. One way to solve the problem is to require the WLAN system to extend its confidentiality and integrity services to the access server. The access server is a device assumed to have some physical access security and therefore better suited to

*Privacy has many aspects; one of them is location privacy. Location privacy is problematic since there often is a strong connection between the logical identity of the user and the routable address associated with the user device.*

[2] *Note that it is permissible to use an EAP method called GSM SIM [12] for GSM subscribers who do not have a UICC. See TS 33.234 [8, Sec. 6.1.2] for more details.*

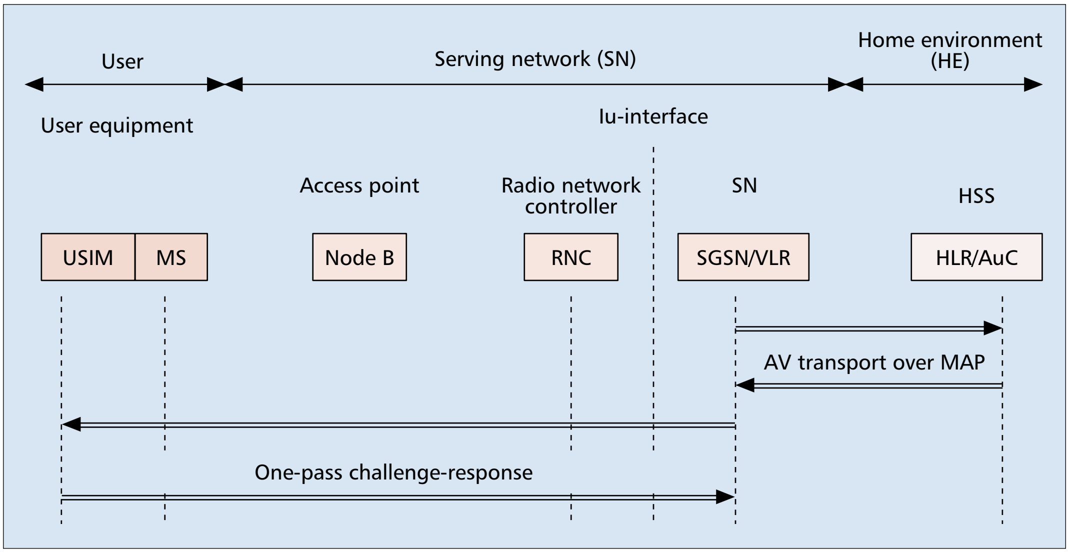


**Figure 2.** *Overview of the UMTS AKA sequence.*

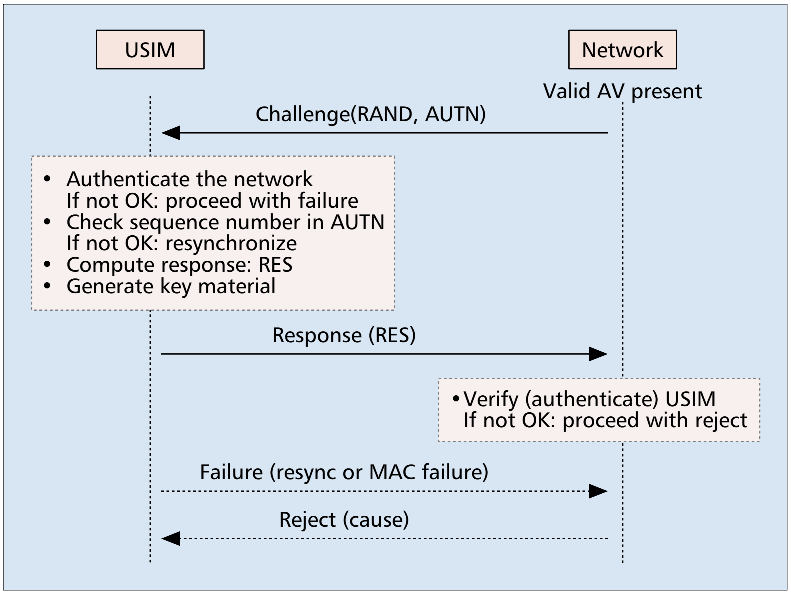

USIM
Network
Valid AV present
Challenge(RAND, AUTN)
• Authenticate the network
If not OK: proceed with failure
• Check sequence number in AUTN
If not OK: resynchronize
• Compute response: RES
• Generate key material
Response (RES)
• Verify (authenticate) USIM
If not OK: proceed with reject
Failure (resync or MAC failure)
Reject (cause)

**Figure 3.** *The UMTS AKA challenge-response mechanism.*

store the session keys. We also note that UMTS has protected data connections between the UE and the radio network controller (RNC) (Fig. 2).

Generally speaking, the security services provided by a wireless system for over-the-air protection are implemented at the link layer. Apart from solving the pressing issue of over-the-air protection, this approach is locked to the specific link layer mechanism. This is also the case for the IEEE 802.11 WLAN system.

So if one wants the security services to extend beyond the AP, one must seek a solution above the link layer. One solution is to create an IPsec tunnel between the UE and the NAS. Such a solution has the drawback of requiring extra client side configuration. There are also scenarios where the home network wants more control, and one may set up a protected tunnel from the UE to the WLAN access gateway (WAG) in the home network.

## Standardization of Security for 3G-WLAN Interworking

### The UMTS Authentication and Key Agreement Protocol

The security architecture of 3GPP-WLAN interworking in UMTS is directly modeled on the UMTS security architecture for access security. Access security in UMTS [14] is based on a one-pass mutual entity authentication scheme executed between the user (USIM) and the SN. In addition to providing authentication, the AKA procedure also includes generation of session keys for confidentiality (128-bit) and integrity (128-bit) protection.

In the UMTS system the AKA procedure is executed in two phases (Fig. 2). The first phase involves transfer of authentication vectors (AVs) from the HE to the SN. This part of the UMTS AKA procedure is not found in the 3GPP-WLAN interworking version of the AKA scheme. The reason is that one does not delegate responsibility for authentication to the SN for 3GPP-WLAN access. Instead, one executes the AKA globally from the HE toward the USIM. In the UMTS only scenario, the second AKA phase is where the SN executes the AKA procedure (Fig. 2).

For the UMTS scenario the HE delegates responsibility for the authentication to the SN. For the 3GPP-WLAN interworking scenario the AKA procedure is executed globally. The drawback is that the signaling paths and thus the round-trip delay may increase. The advantage is improved home control since there is no need to distribute AVs or authentication control to the SN.

The cryptographic functions used in the AKA procedure are only implemented in the USIM and HSS, and are thus only dependent on the HE operator. The outcome of a successful AKA sequence is that the USIM and network will be mutually authenticated, and will have derived common key material.

The AKA may occasionally fail. The USIM

may find the *challenge* to be invalid and therefore reject the network. Conversely, the SN may receive an invalid *response* from the USIM and therefore reject the USIM. In addition, the AKA protocol may also fail due to the use of expired security credentials. This event is treated as a synchronization failure, and one can recover through a resynchronization procedure. A more detailed description of the UMTS AKA procedure specifics can be found in [14, 15] (Fig. 3).

### The 3GPP-WLAN Security Architecture

A benefit of the loose interworking approach is that the 3GPP-WLAN architecture is a fairly simple architecture. The architecture contains the WLAN access network and a UMTS core network in addition to glue technology to connect the two systems. Figure 4 gives an overview of the proposed architecture.

The two key glue components of the interworking solution are the AAA and EAP technologies. These are used to execute the UMTS AKA protocol from the 3G system's home domain toward the WLAN user equipment.

The AAA architecture and the RADIUS and/or Diameter protocol are to be used as the bridge between the 3GPP system and the WLAN access network. The EAP-AKA [12] protocol allows the UMTS AKA security protocol, which was originally designed for execution over UTRAN, to be executed over the WLAN access toward the user equipment.

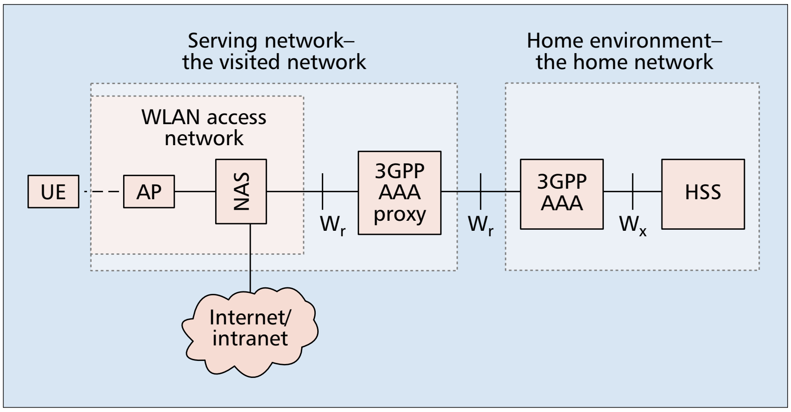


**Figure 4.** *Simplified 3GPP-WLAN architecture.*

### The Role of the Extensible Authentication Protocol

EAP [10] is a key element in the 3GPP-WLAN security architecture. EAP provides, in essence, a generic peer-to-peer based *request-response* transaction environment for authentication dialogs, and supports multiple authentication mechanisms.

EAP typically runs directly over the link layer without requiring IP. EAP has its own flow control mechanisms, and is capable of removing duplicate messages and retransmitting lost messages. EAP can be used over different link layer protocols including the IEEE WLAN link layer. The necessary EAP encapsulation is described in the EAP-over-LAN specification [11].

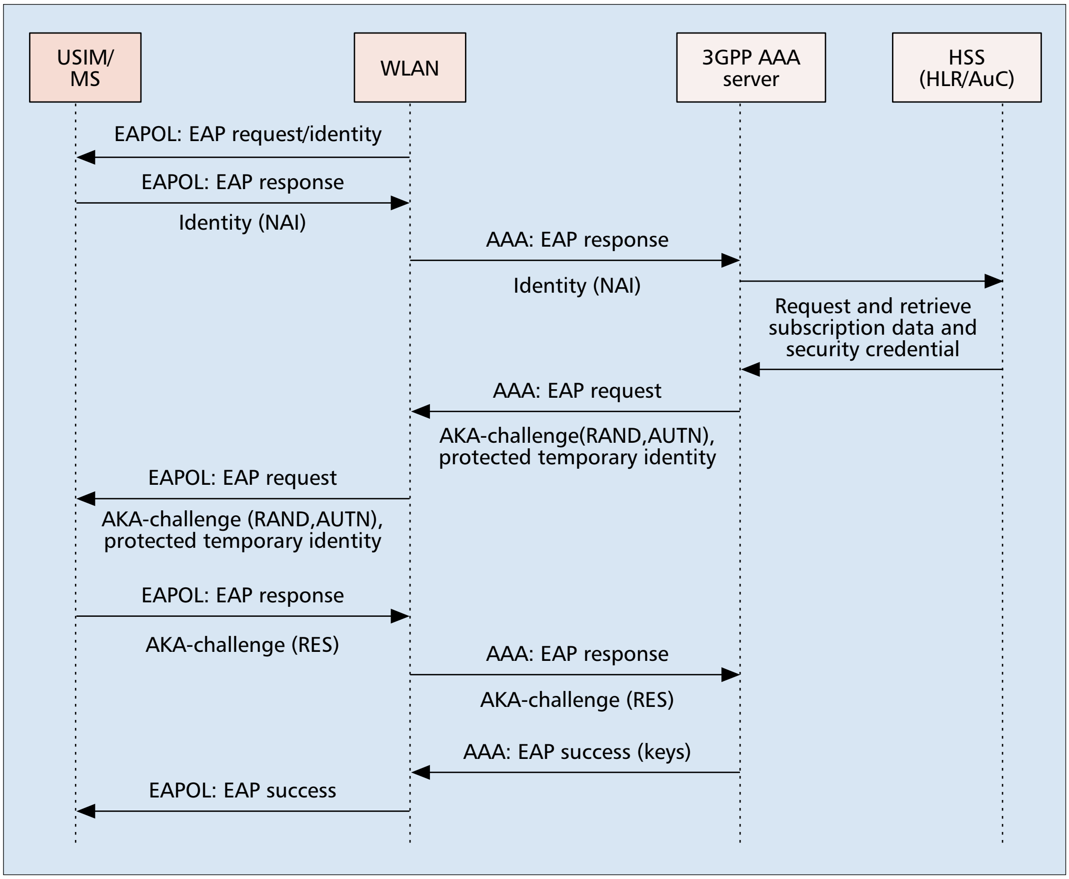


**Figure 5.** *A successful UMTS AKA procedure (simplified) between a 3GPP network and an 802.11 WLAN MS.*

*Despite some challenges, the future looks bright for 3GPP-WLAN interworking, and the security provided will benefit the user as well as the system operators.*

The EAP protocol does not natively provide much in terms of authentication mechanisms. Instead, its power lies in its generic mechanism to support existing authentication methods through specialized EAP methods. EAP contains a negotiation sequence where the authenticator requests information about which authentication method to use. The EAP architecture does not require the authenticator to support all authentication methods. Instead, the authenticator can request assistance from a backend authentication server to complete the authentication processing.

The specific authentication methods supported are defined in separate specifications detailing how the EAP framework is to be used to run the target authentication methods. For 3GPP-WLAN interworking, we are primarily interested in the EAP-AKA [12] methods.

Successful execution of the EAP-AKA procedure specific to the IEEE 802.11 WLAN is illustrated in Fig. 5.

### AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

To manage roaming traffic, the AAA framework is chosen as the basis for the 3GPP-WLAN architecture. As used in the 3GPP-WLAN setting, the AAA architecture is quite simple.

The AAA protocol proposed is the Diameter protocol, but RADIUS will also be allowed from the 3GPP system toward the WLAN system. Both Diameter and RADIUS are generic protocols and are intended to provide support for a diverse set of AAA applications, including network access, IP mobility, and interoperator roaming.

All AAA data delivered is in the form of attribute-value pairs (AVPs). Some of the AVP values are used directly by Diameter/RADIUS, while others carry data associated with a particular AAA application. The AAA applications are domain -specific and define their own sets of AVPs. To be able to use EAP-AKA, one needs the AAA EAP application.

## SUMMARY AND CONCLUSION

The idea of interworking between mobile systems and WLANs holds great promise. From the cellular world one inherits near universal access, a roaming infrastructure, security management, and a charging regime. From the WLAN side one get high bit rates and hot spot coverage at a reasonable cost. Security-wise the interworking is mostly unproblematic, but there are areas identified that contain weaknesses.

One issue that needs to be investigated further is the need for even better identity protection. Identity privacy is important and will probably become even more important in the future as technology advances.

Despite some challenges, the future looks bright for 3GPP-WLAN interworking and the security provided will benefit the user as well as the system operators.

## REFERENCES

[1] IEEE Std 802.11b-1999, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Higher-Speed Physical Layer Extension in the 2.4 GHz Band."

[2] IEEE Std 802.11a-1999, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; High-Speed Physical Layer in the 5 GHz Band."

[3] P. S. Henry and H. Luo, "WiFi: What's next?," *IEEE Commun. Mag.*, vol. 40, no. 12, Dec. 2002

[4] ETSI TS 101 475 v. 1.1.1, "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Physical (PHY) Layer."

[5] ETSI BRAN30d135r1 and IEEE 802.11 03-005, WIG baseline doc.

[6] IEEE Std 802.11i/D4.0, "Draft Amendment to Standard for Telecommunications and Information Exchange Between Systems — LAN/MAN Specific Requirements — Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Control (MAC) Security Enhancements," May 2003, work in progress.

[7] ETSI TR 101 957, "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Requirements and Architectures for Interworking between HIPERLAN/2 and 3rd Generation Cellular Systems."

[8] 3G TS 23.234, "3GPP System to Wireless Local Area Network (WLAN) Interworking System Description," Release 6, work in progress.

[9] 3G TS 33.234 v050, "3G Security; Wireless Local Area Network (WLAN) Interworking Security," Release 6, work in progress.

[10] L. Blunk *et al.*, "Extensible Authentication Protocol (EAP)," Internet draft, draft-ietf-eap-rfc2284bis-04.txt, June 2003, work in progress.

[11] IEEE Std. 802.1X-2001, "IEEE Standard for Local and Metropolitan Area Networks — Port-Based Network Access Control," July 2001.

[12] J. Arkko and H. Haverinen, EAP AKA Authentication, Internet Draft: draft-arkko-pppext-eap-aka-10.txt, June 2003, work in progress.

[13] H. Haverinen and J. Salowey, "EAP SIM Authentication," Internet draft, draft-haverinen-pppext-eap-sim-11.txt, June 2003, work in progress.

[14] 3G TS 33.102, "3G Security; Security Architecture."

[15] G. M. Køien, "An Introduction to Access Security in UMTS," to be published, *IEEE Wireless Mag.*

## BIOGRAPHIES

GEIR M. KØIEN (Geir.Koein@hia.no) is the Telenor delegate to 3GPP TSG SA3 (Security). He is currently partly on leave to pursue a Ph.D. at the University of Aalborg, Denmark. His primary research interest is in formal aspects of security and mobility issues.

THOMAS HASLESTAD has been the Telenor delegate to ETSI BRAN, where he was the chair of the ETSI BRAN 3G Interworking Group. He is also former co-chair of the Wireless Interworking Group (WIG).