Network Smart Card Performing U(SIM) Functionalities in AAA Protocol Architectures

Joaquin Torres, Antonio Izquierdo, Mildrey Carbonell, and Jose M. Sierra

Carlos III University of Madrid, Spain
Computer Science Department
{joaquin.torres,antonio.izquierdo,mildrey.carbonell,jm.sierra}@uc3m.es

Abstract. This paper reviews the way in which the security protocols EAP-SIM/AKA are used in 3G/WLAN network interworking from the point of wiew of the U(SIM). As result, a new AAA protocol architecture is derived from the integration of a Network Smart Card, NSC, that implements U(SIM) functionalities within the scheme. The implementation in a testbed shows the robustness and feasibility of such an architecture.

Keywords: Network smart cards, authentication and authorization architectures, WLAN/3G interworking, secure protocols.

1 Introduction

The wide availability of wireless equipments of reduced size increases the demand for access points to the worldwide digital information and services. Although initially WLANs were conceived as an extension of corporative networks, nowadays their usage has been popularized in SOHO, campus and residential environments. The number of public hotspots is continuously proliferating, and this allows the information to be accessible in any time and any place.

The third generation mobile systems could be seen as a competitive solution, in terms of wide geographical area coverage and effective roamings. Moreover, depending on the scenario, issues such as reliability, throughput, value-added services (e.g. global localization) and contents (including multimedia services directly to your mobile phone) should be considered as advantages that this technology could offer. However, the expensive investment required by the 3G networks forces to the operators to look for more profitable and versatile solutions, and aiming to offer a wider variety of services for avoiding a leakage of subscribers.

WLAN's features allow to provide services with significant transmission rates in high demand zones and when the mobility is not a requirement. On other hand, 3G systems offer high mobility, wide coverage, well-established voice services but lower transmission rates, so they are more adequate for low/medium demand. Additionally, these systems posse a robust network and management infrastructure to deal with demands for security, billing and roaming requisites. Thus, as it is shown, wireless local area and 3G networks are complementary.

J.A. Onieva et al. (Eds.): WISTP 2008, LNCS 5019, pp. 92–105, 2008.

The wireless local area and 3G cellular networks interworking is a clear trend in the public access infrastructures (*PWLAN , Public Wireless LAN*) [1], which are progressively being deployed. It is considered as a significant step towards the fourth generation of all-IP wireless networks.

The combination of both technologies are allowing the development of services with high transmission rates (e.g. IP-based multimedia services, IMS) in mobile/roaming scenarios for an important number of profiled subscribers and preserving the quality of services. Beyond multimode terminals that provide both wireless interfaces (3G and WLAN) in order to access to each system, there exist integral solutions that provide transparent roaming between both technologies by the appropriate smart switching, with the goal of keeping initiated sessions.

In the 3G/WLAN integration, the subscriber must be authenticated before being her access to network services authorized. Thus user's multimode devices (e.g. laptops, smartphones, PDAs, etc.) require the appropriate personalized secure module. As in the stand-alone 3G systems, the chip card-based U(SIM) provides this functionality in PWLANs.

The important role of smart cards in this context is worth studying if one considers potential scenarios with the corresponding security functionalities. In Figure 1, an independent smart card with authentication purposes is isolated in the reference model.

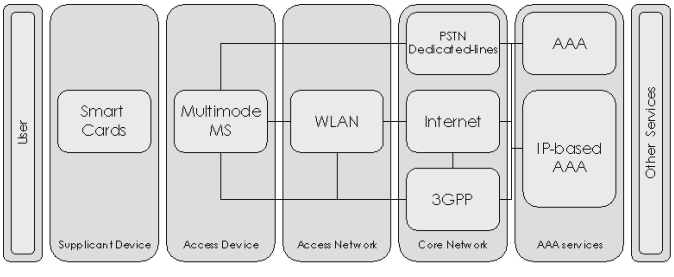

Fig. 1. Reference Model

In the 3G/WLAN interworking, the authentication schemes are based on a combination of the solutions that were initially supported by these two systems: the SIM-based solutions simultaneously inherit from EAPoL-based (i.e. 802.1X/EAP, RADIUS [2][3] or DIAMETER [4] used in WLAN technologies) and from U(SIM) authentication schemes supported by 3GPP subscriber registers (i.e. HLR/HSS).

The standardized protocols EAP-SIM [5] and EAP-AKA [6] represent the two most relevant SIM-based authentication schemes that establish mutual authentication between the mobile station and the backend authentication server. On one hand, the user is accustomed to use an (U)SIM, which allows her to access to a set of services by means of her mobile phone. On the other hand, the 3G/WLAN network operators do not require a different credential or secure module in order to authenticate, personalize or bill for such services. Hence, the

SIM-based authentication schemes are good competitors against the Web-based schemes, among other reasons due to the latter does not provide mutual authentication functionality between mobile station and backend server (a client certificate should be required) whereas the SIM-based schemes easily supports such a functionality.

Consequently, the EAP-SIM/AKA standardized protocols along with RADIUS or DIAMETER (supporting AAA procedures) are de facto authentication schemes for the 3G/WLAN interworking architectures [7][12]. By means of a number of proxies, it is possible to transport the authentication messages through a visited wireless local network towards our home 3GPP network, in a roaming situation.

Due to the complexity associated to the network in 3G/WLAN scenarios, most of works have been focused on the security and technical problems in the network side. Thus, some authors highlight the resulting latency during the authentication process and propose techniques based on AAA brokers as third trusted party [8], which manages the security associations and key distribution. Other original works are focused on a proactive key distribution scheme based on a context transfer between foreign and home network [9], and in other cases, as we will see in the section 2 of this paper, they study global security problems associated to the standardized protocols.

Nevertheless, regarding the chip card running in these interworking schemes in a U(SIM) role, few works have been developed and that is the scope of the present paper. More concretely, this paper aims to review the way in which the EAP-SIM/AKA security protocols are used in 3G/WLAN interworking from the point of view of U(SIM), with the goal to provide a more robust and secure solution.

Our new approach starts from a different authentication model [10] that considers an isolated U(SIM) with autonomy during the authentication process. In other words, the U(SIM) participates as stand-alone supplicant or claimant, and not relies on the access terminal (i.e. WLAN mobile station) for this functionality. Additionally, this work assumes an a priori untrustworthy environment, where the WLAN MS is considered as a potential attacker. Hence, the WLAN MS should be authenticated by the network as a different host from U(SIM). Thus, we will define in this paper an AAA architecture, which represents a more robust and flexible solution in terms of security. Beyond these benefits, this approach also provides efficient mobile stations' customization or personalization in critical or public environments.

In the reminder of this paper, the related work is reviewed in section 2 and, afterwards, we describe an AAA architecture based on our network smart card concept [10], NSC, which implements U(SIM) authentication functionalities (NSC-based U(SIM)). In section 4, security and trust issues related to such an architecture are discussed. Finally, we describe the testbed and implementation carried out with the goal to run end-to-end authentication protocols over the proposed architecture and to test her feasibility.

2 Related Work

The advances in the 3G/WLAN interworking systems have been reflected in the standardization process [7][11], where the reference model for different scenarios is detailed. In [12] and other works [13] [14], the security related to theses systems is profusely described. An example of interworking architecture (compounded by UMTS and IEEE802.11 technologies) was evaluated in simulation environments in [15].

After the subscriber authentication phase takes place by means of her U(SIM), the cellular network operator will provide access to certain IP-based services. It is important to highlight the heterogeneity feature in wireless devices and networks under the all-IP concept, which is applied along the end-to-end communication for the provision of multiple services (Web, IMS, VoIP, video streaming, etc.). From the beginning, many works were devoted to this topic. In [16], the call admission control over various DiffServ settings was studied for this kind of architectures and in [17] the session establishment with SIP was tested for the provision of IMS services. In [18] the VoIP throughput into an IPSec tunnel was analysed by forcing the number of connections to an unique access point in mobility situations.

Continuing with the network side, standards and many works have been focused on 3G/WLAN interworking security. The subscriber authentication process (more general, AAA) through the 3G/WLAN architecture in a roaming situation and, obviously, previous to the IP session, is illustrated in Figure 2. A wireless local network based on IEEE 802.11i technology is represented.

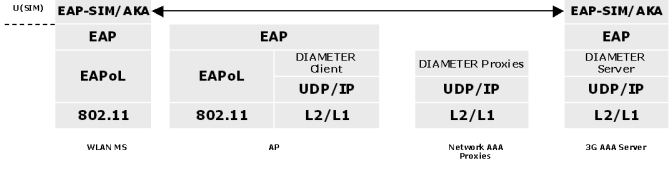

Fig. 2. Example of an AAA protocol architecture in 3G/WLAN interworking

The AAA architecture shown in Figure 2 is based on the EAP-SIM/AKA protocols. In summary, the U(SIM) stores the corresponding subscriber authentication credentials and computes the envisaged cryptographic algorithms in such protocols, on the behalf of mobile station. In order to provide universal support for transmission-level security, and enable both intra- and inter-domain AAA deployments, IPsec support is mandatory in DIAMETER [19][4]. IPsec ESP in transport mode and authentication algorithms provides per-packet authentication, integrity protection, confidentiality and supports replay protection mechanisms.

Nevertheless, some weaknesses in EAP-SIM/AKA schemes have been found [20][21][22]. Since authentication procedure requires multiple request-response

exchanges, attacks in visited networks that can compromise authentication vectors in roaming situation have been detected. Moreover, identity privacy is not always guaranteed when the identification of a user is performed by means of the permanent subscriber identity (IMSI) or pseudonym in clear text [23]. Additionally, the system could be actively attacked by a malicious impersonation of the network with the goal to obtain the subscriber's IMSI. Finally, EAP-AKA does not support cipher suite negotiation or protocol version negotiation , therefore negotiation attacks are feasible, as well as, man-in-the-middle attacks.

With the goal of overcoming these flaws, in [21] and more recently in [24] can be found proposals of tunnelled end-to-end authentication schemes based on EAP-TLS [25] or EAP-TTLS [26] over the 3G/WLAN interworking architecture. Other previous working lines, have aimed to make more robust the subscriber authentication and authorization on the basis of temporary attributes certificates [27]. The goal of this proposal was to reduce the inconveniences of the certificates management and their revocation, minimizing the impact on the interworking architecture.

However, the problems derived from the certificate management in the client side or/and from the complexity of tunnels establishing, supported by the U(SIM), suggest to look for more lightweight schemes.

Another problem in the current implementation of EAP protocols in U(SIM) is due to the by default consideration of a implicit trustworthy WLAN MS (e.g. laptop, smartphone, PDA, etc.). That means that both devices blindly trust each other. In fact, they behave as an unique supplicant. In our opinion, this is not a by default recommendable assumption. Thus, the authentication schemes should be designed to protect against any potential scenario, even where the WLAN MS is an a priori untrustworthy terminal.

Moreover, when a smart card interacts in an untrustworthy environment, a previous devices authentication (UICC and mobile station) should be required before a secure messaging (ISO 7816) is established. However, this protection is not considered in [12], as it is illustrated in Figure 2.

Therefore, a more robust approach should be performed in order to obtain versatile solutions. Just note that, an U(SIM) may be an external contact/contacless smart card that customizes (personalizes) a public wireless terminal for a 3G/WLAN access. Specifically in such a case, the U(SIM) behaviour as an stand-alone supplicant is highly recommendable. So it should be isolated and protected. Otherwise, the WLAN MS could be considered as the perfect candidate to be the man in the middle. An example of MitM attack concerning EAP-SIM is described in [28]. This attack breaks the A5/2 algorithm, whenever a few valid GSM triplets have been retrieved.

In the following section, we propose a novel approach on the AAA architecture in Figure 2. This proposal is respectful with the required protocols (EAP-SIM/AKA, RADIUS/DIAMETER, etc.) and it basically aims to improve the robustness and security in this kind of interworking scenarios.

3 New NSC-Based AAA Protocol Architecture in 3G/WLAN

This paper proposes a new AAA protocol architecture for 3G/WLAN infrastructures based on our Network Smart Card concept (NSC-based). Under this scope, we consider an U(SIM) remote authentication scheme, where this device adopts the functionality of stand-alone supplicant instead of split supplicant: the U(SIM) and WLAN MS does not cooperate in the authentication process as an unique device. That is why, in our work, the authentication protocol stack is designed as an integral part of the U(SIM) (atomic design). With this goal, we propose a specific protocol stack for the chip card that participates as actual endpoint in the authentication process with a 3G AAA server.

This new architecture (Figure 3) implies minimal changes in the original one (Figure 2) but it introduces significant advantages. For instance, in the 3G network side no changes are needed. Thus, proxies and end-equipments keep settings and implementation features.

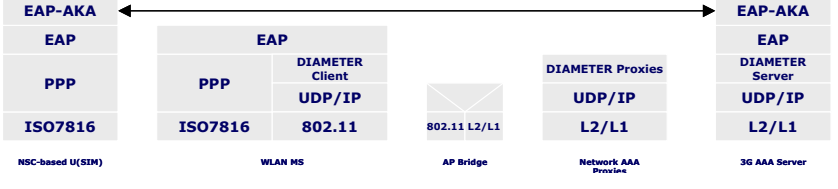

Fig. 3. Our NSC-based AAA protocol architecture in 3G/WLAN interworking

The proposed AAA protocol architecture requires a simpler protocol implementation for the WLAN acces points (APs) with U(SIM) remote authentication purposes. Note that WLAN Mobile Station participates as a Network Access Server (NAS) implementing the role of pass-through authenticator as a DIAMETER client according to [4].

In a first phase, the DIAMETER server authenticates the WLAN MS by her own mechanisms. In a second phase, the function of the pass-through authenticator is shifted to WLAN MS. This reinforces the stand-alone supplicant functionality in the U(SIM), since WLAN MS cannot act as supplicant and authenticator at the same time for the same U(SIM). One should note the advantages that the U(SIM) isolation brings with regard to assure the security of the entire scheme in untrustworthy scenarios.

Our architecture takes advantage of the functions of the LCP protocol that is provided by PPP [29]. LCP/PPP protocol may be easily hosted in the U(SIM) stack. The functions for controlling network included in the NCP sub-protocol are beyond the scope of this work. On the other hand, PPP offers versatility in the authentication, thanks to its extensibility. In fact, EAP (Extensible Authentication Protocol) was initially designed for PPP. According to our approach, the EAP Layer must be atomically implemented in the smart card and must allow

the packets exchange between the EAP-SIM/AKA methods and LCP frames, as well as, the duplication and retransmissions control.

Based on this architecture, an authentication messages exchange has been designed in our work. Figure 4 illustrates this authentication flow.

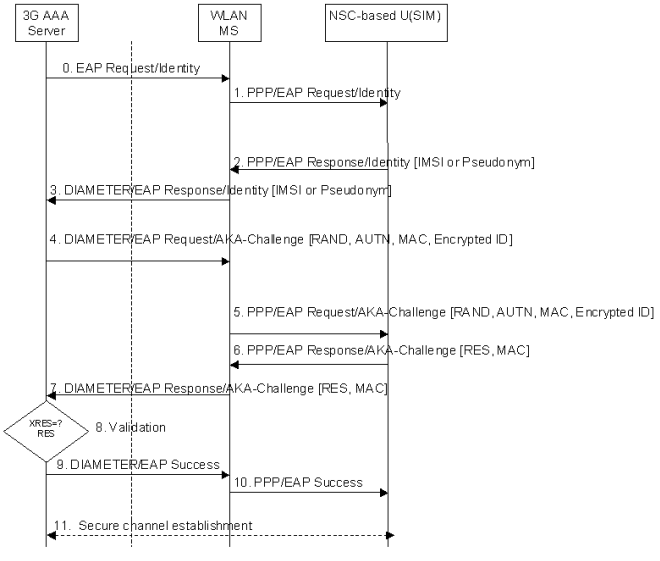

Fig. 4. Authentication Flow in our AAA architecture

The NSC-based U(SIM) authentication process is as follows:

1. The WLAN MS (representing the network and providing WLAN access) sends an PPP-EAP request identity (either an IMSI or a pseudonym) message to the NSC-based U(SIM) in order to initiate the procedure.

2. The NSC-based U(SIM) returns the EAP Response/Identity packet to the WLAN MS.

3. The WLAN MS sends the EAP Response/Identity packet to the 3G AAA Server in network. The authentication messages exchange between WLAN MS and 3G AAA Server are encapsulated into DIAMETER packets.

4. The 3G AAA Server initiates the EAP AKA authentication process with the appropriate EAP Request/AKA-Challenge message.

5. The WLAN MS processes the DIAMETER headers and sends the received EAP packet to the NSC-based U(SIM), encapsulated into a PPP frame.

6. The NSC-U(SIM) returns the EAP Response/AKA-Challenge packet to the 3G AAA Server, which will check the validity of the RES.

7. The WLAN MS builds the corresponding DIAMETER packet and sends it to the 3G AAA Server.

8. The 3G AAA Server checks the validity of the RES and computes the MAC of the entire received message, and she compares it with the received MAC.

9. In case of a correct validation, the NSC-based U(SIM) is authenticated and the 3G AAA Server sends an EAP Success packet to the NSC-based U(SIM).

10. The WLAN MS retransmit the EAP Success packet on the PPP link.

11. After a successful EAP authentication, the NSC-based U(SIM) is authorized by the network equipment (e.g., WLAN MS or even the actual 3G AAA server). Both devices could derive/know a master session keys to establish a secure channel (secure messaging) between them.

As is stated in [7], an EAP-AKA fast re-authentication procedure was developed with the goal to make more lightweight the authentication process. Note that the EAP-AKA authentication process may be frequently performed in order to obtain fresh authentication vectors from the home network. By means of fast re-authentication procedure, the certain keys that have been derived in a previous full authentication are reused, so just one new master session key is generated with link layer protection purposes. The inclusion of the EAP-AKA fast re-authentication in our scheme is trivial.

4 Security and Trust Issues

Regarding the security aspects of our architecture, it should be noted that we are not proposing a new U(SIM) authentication protocol in the context of 3G/WLAN interworking. Our architecture is designed by well-known protocols that are implemented inside the U(SIM) with a novel approach.

Nevertheless, this new architecture determines a new way to transport authentication messages between the U(SIM) and a 3G AAA server, and where the U(SIM) takes the control in the user side. Therefore, the security weakness and threats are derived by the own nature of such standardized protocols and the correctness of their implementation.

Additionally, new secure algorithms, key material or cryptographic techniques are not required. The implementation of the EAP-SIM or EAP-AKA methods is transparently reused, both in the U(SIM) side and in the 3G AAA Server side. However, one of the more important impacts of our proposal is related to the trust models. If we study the trust model, Figure 5, derived from the current AAA protocol architecture in a 3G/WLAN interworking scenario (Figure 2), we

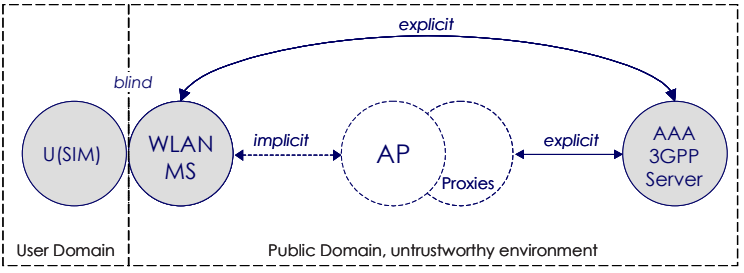

Fig. 5. Trust model in the original architecture

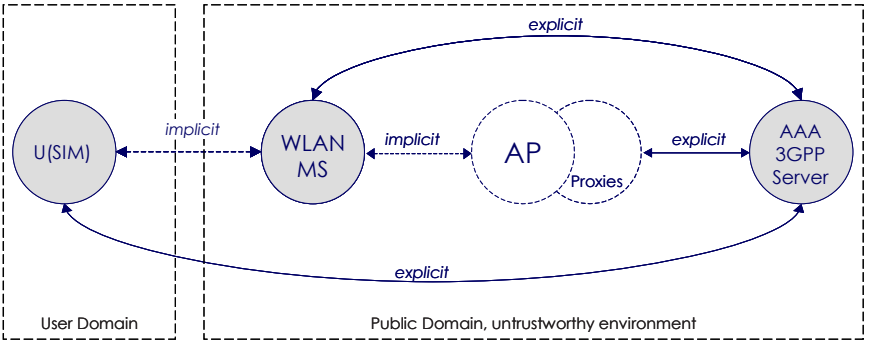

Fig. 6. Trust model in our architecture

observe that there exists an explicit trust between AP and 3GPP AAA server (supported by DIAMETER protocol) and an explicit trust between WLAN MS and 3GPP AAA server after a successful authentication process (supported by an EAP method). In any case, the trust relationship in the interface between U(SIM) and WLAN MS is not questioned and it could be considered as "blind". As we mentioned before, this assumption should not be applied to all scenarios and a more flexible solution is required. With this goal, we introduce a more realistic architecture, which a new trust model is derived from, Figure 6.

In our trust model, the trust relationship between the WLAN MS and the 3G AAA server is supported by DIAMETER protocol (e.g pre-shared keys) and such trust relationship could be considered as explicit. Here, the WLAN MS is part of the network and it behaves as an access point for the U(SIM). The trust relationship between U(SIM) and WLAN MS is a priori null (untrustworthy). After an end-to-end successful authentication process (supported by an EAP-SIM/AKA method) between the U(SIM) and 3G AAA Server, the trust relationship between them should be now considered explicit, as result of a mutual authentication process. Therefore, in this point the trust relationship between U(SIM) and WLAN MS is just implicit, since no direct mutual authentication process between them has occurred. In other words, just when U(SIM) trusts 3G AAA server then she trusts WLAN MS. This is a reasonable result in a priori untrustworthy scenarios.

Moreover, in untrustworthy scenarios a device authentication process should occur, i.e. an authentication process between devices based on shared keys (or card verifiable certificates), directly driven by the involved devices. In this context, it does not make sense to perform two mutual remote authentication, i.e. subscriber authentication and device authentication, so a local device authentication (U(SIM)- WLAN MS) may take place in order to avoid an additional management of the key material in a number of public WLAN MSs. By means of our AAA protocol architecture the corresponding master session key (also derived by U(SIM)) is sent to WLAN MS from the network side. Therefore, the (U)SIM-WLAN MS interface is per-session authenticated and protected against potential attacks (e.g. MitM attack, WLAN MS impersonation).

Although some flaws in EAP-AKA have been proved by several authors, the tunnel-based solutions (e.g. based on EAP-TLS) are interesting proposals, which could deal with these weaknesses. In principle, our architecture could further implement this kind of protocols, though performance tests should be carried out.

5 Implementation and Testbed

The testbed for the AAA network architecture is represented in Figure 7. It has been implemented by means of the OpenDiameter [30] libraries. OpenDiameter libraries provide a C++ API both to EAP and Diameter EAP.

3G AAA Server

The back-end authentication server is basically implemented in a computer by the *libdiametereap* library. Such a library implements the specification defined in [4]. The Diameter EAP API is extensible in a way that server applications can define its own authorization decisions for each authorization attribute carried in Diameter EAP Answer (DEA) messages.

Additionally, the *libeap* library implements a set of state machines of EAP, which is specified in [31] . In this case, this library provides an EAP backend authenticator implementation.

The EAP API is extended in order to support EAP-AKA as a new authentication method including the corresponding method's state machine and message parsing. On the other hand, the *OpenSSL* library includes a general purpose cryptography library, which is partially included in this testbed with the goal of providing a set of AKA cryptographic functionalities. Since this work is focalised on authentication purposes, for simplicity's sake, the implementation of functions f3 and f4 [32] has not been carried out. This functions are envisaged with key agreement purposes (CK and IK). These keys would be used to derive further keying material with different goals: e.g. EAP-AKA additional packets protection, link layer security, in HMAC algorithm or fast re-authentication identity encryption.

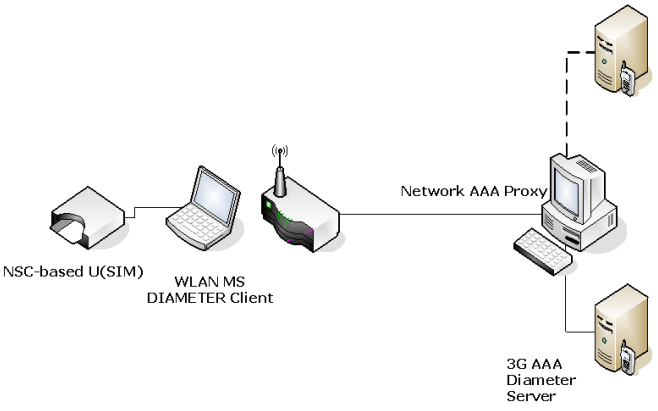

Fig. 7. Testbed for our architecture

Network AAA proxy

Multiple network AAA proxies could intermediate between the wireless LAN network and the 3G network. Our testbed considers just one proxy, which simulates one of these entities. The standard Diameter base protocol procedure in her relay version (Diameter proxy) is provided by the *libdiameter*. It allows us to complete the implementation of the adequate protocol stack in a layer 2 wireless Access Point. In our testbed, Diameter messages are hop-by-hop protected by IPsec with pre-shared keys (IKE Aggressive Mode) between WLAN MS (NAS), AAA proxy and between this one and AAA server.

WLAN MS

The WLAN mobile station is a common laptop with a IEEE 802.11g wireless interface. The functionality of NAS (Diameter client) is provided by the implementation of the *libdiametereap* library.

Network Smart Card with U(SIM) functionalities

The base implementation in the smart card for this testbed is previously described in [10]. Thus, the bulk LCP/EAP protocol stack -according to the standardized state machines- has been enhanced with a set of functionalities corresponding EAP-AKA method. As is stated before, CK and IK derivation, as well as, synchronization and re-authentication functionalities have been avoided with testbed experiments purposes. Partial view of the EAP- AKA state machine is illustrated in Figure 8.

Although we are continually improving the implementation of this architecture and protocol, we have measured a initial performance time of 6-7 sec. for completing the authentication process (authorization policy is excluded) in laboratory environment. The Sm@rtCafé Expert 3.x and Sm@rtCafé Expert 64 smart cards and G&D's development tools [33] have been used for the experiments in our testbed.

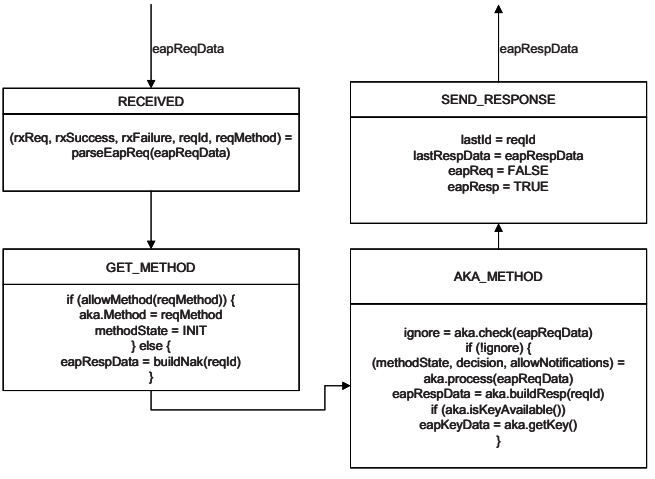

Fig. 8. Partial view of the EAP state machine in the smart card

6 Conclusion

Our testbed shows the feasibility and robustness of the proposed NSC-based AAA protocol architecture for 3G/WLAN interworking scenarios. The standardized EAP-AKA protocol is transparently implemented in a common U(SIM), which participates as stand-alone supplicant (NSC-based U(SIM)), and she does not rely on the WLAN mobile station for this functionality. This feature defines a novel trust model that assumes an a priori untrustworthy environment, where the WLAN MS is considered as a potential attacker. Thus, our approach represents a more flexible solution in terms of security. Beyond these benefits, it also provides efficient mobile stations' customization or personalization in critical or public environments. Next future works will study other related protocols over the same architecture and they will in depth treat performance tests.

Acknowledgements. This work is supported by ASPECTS-m Project, CICYT-2004-SEG-04000.

References

1. Leu, J.-S., Lai, R.-H., Lin, H.-I., Shih, W.K.: Running cellular/PWLAN services: practical considerations for cellular/PWLAN architecture supporting interoperator roaming. IEEE Communications Magazine 44(2), 73–84 (2006)
2. Rigney, C., Willens, S., Rubens, A., Simpson, W.: Remote Authentication Dia. In: User Service (RADIUS), IETF RFC 2865 (June 2000)
3. Aboba, B., Calhoum, P.: RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), IETF RFC 3579 (September 2003)

4. Eronen, P., Hiller, T., Zorn, G.: Diameter Extensible Authentication Protocol (EAP) Application, IETF RFC 4072 (August 2005)
5. Haverinen, H., Salowey, J.: Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM), IETF RFC 4186 (January 2006)
6. Arkko, J., Haverinen, H.: Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), IETF RFC 4187 (January 2006)
7. 3GPP TS 23.234 v7.3.0: 3GPP System to Wireless Local Area Network (WLAN) Interworking System Description (September 2006)
8. Salgarelli, L., Buddhikot, M., Garay, J., Patel, S., Miller, S.: Efficient authentication and key distribution in wireless IP networks. IEEE Wireless Communications 10(6), 52–61 (2003)
9. Shin, M., Ma, J., Mishra, A., Arbaugh, W.A.: Wireless network security and interworking. Proceedings of the IEEE 94(2), 455–466 (2006)
10. Torres, J., Izquierdo, A., Sierra, J.M.: Advances in network smart cards authentication. Computer Networks 51(9), 2249–2261 (2007)
11. Ahmavaara, K., Haverinen, H., Pichna, R.: Interworking architecture between 3GPP and WLAN systems. IEEE Communications Magazine 41(11), 74–81 (2003)
12. ETSI TS 133 234 V7.5.0, 3GPP System to Wireless Local Area Network (WLAN) Interworking Security System (June 2007)
13. Koien, G.M., Haslestad, T.: Security aspects of 3G-WLAN interworking. IEEE Communications Magazine 41(11), 82–88 (2003)
14. Salkintzis, A.K.: Interworking techniques and architectures for WLAN/3G integration toward 4G mobile data networks. IEEE Wireless Communications 11(3), 50–61 (2004)
15. Siddiqui, F., Zeadally, S., Yaprak, E.: Design Architectures for 3G and IEEE 802.11 WLAN Integration. In: Lorenz, P., Dini, P. (eds.) ICN 2005. LNCS, vol. 3421, pp. 1047–1054. Springer, Heidelberg (2005)
16. Song, W., Jiang, H., Zhuang, W., Shen, X.: Resource management for QoS support in cellular/WLAN interworking. IEEE Network 19(5), 12–18 (2005)
17. Marquez, F.G., Rodriguez, M.G., Valladares, T.R., de Miguel, T., Galindo, L.A.: Interworking of IP multimedia core networks between 3GPP and WLAN. IEEE Wireless Communications, [see also IEEE Personal Communications] 12(3), 58–65 (2005)
18. Rajavelsamy, R., Jeedigunta, V., Holur, B., Choudhary, M., Song, O.: Performance evaluation of VoIP over 3G-WLAN interworking system. IEEE Wireless Communications and Networking Conference 4(13-17), 2312–2317 (2005)
19. Calhoun, J., Loughney, E., Guttman, G., Zorn, J.: Arkko, Diameter Base Protocol, IETF RFC 3588 (September 2003)
20. Barkan, E., Biham, E., Keller, N.: Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication. In: Crypto 2003 (August 2003)
21. Kambourakis, G., Rouskas, A., Kormentzas, G., Gritzalis, S.: Advanced SSL/TLS-based authentication for secure WLAN-3G interworking. IEE Proceedings Communications 151(5), 501–506 (2004)
22. Meyer, U., Wetzel, S.: A man-in-the-middle attack on UMTS. In: Proceedings of the 2004 ACM Workshop on Wireless Security, October 2004, pp. 90–97 (2004)
23. Cheng, R.G., Tsao, S.L.: 3G-based access control for 3GPP-WLAN interworking. In: IEEE 59th Vehicular Technology Conference, VTC 2004-Spring, May 2004, vol. 5, pp. 2967–2971 (2004)

24. Zhao, Y., Lin, C., Yin, H.: Security Authentication of 3G-WLAN Interworking. In: 20th International Conference on Advanced Information Networking and Applications. In: AINA 2006, April 2006, vol. 2, pp. 429–436 (2006)
25. Aboba, B., Simon, D.: PPP EAP TLS Authentication Protocol, IETF RFC 2716 (October 1999)
26. Funk, P., Blake-Wilson, S.: EAP Tunneled TLS Authentication Protocol Version 1, (EAP-TTLSv1), Internet-Draft, draft-funk-eap-ttls-v1-01.txt (March 2006)
27. Kambourakis, G., Rouskas, A., Gritzalis, S., Geniatakis, D.: Support of Subscribers Certificates in a Hybrid WLAN-3G Environment. Computer Networks 50(11), 1843–1859 (2006)
28. Barkan, E., Biham, E., Keller, N.: Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 600–615. Springer, Heidelberg (2003)
29. Simpson, W.: The Point-to-Point Protocol (PPP), IETF RFC 1661, Standard Track (July 1994)
30. Open Diameter Project. Open-source software for the Diameter base protocol and others, `http://www.opendiameter.org/`
31. Vollbrecht, J., Eronen, P., Petroni, N., Ohba, Y.: State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator, IETF RFC 4137 (August 2005)
32. 3GPP TR 35.909 V7.0.0, Technical Specication Group Services and System Aspects; 3G Security; Specication of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation (Release 7) (June 2007)
33. Sm@rtCafé Professional Toolkit 2.0, G&D, `http://www.gi-de.com`