A General IMS Registration Protocol for Wireless Networks Interworking

Daniel Díaz-Sánchez[1], Davide Proserpio[1], Andrés Marín-López[1],
Florina Almenárez-Mendoza[1], and Peter Weik[2]

[1] Universidad Carlos III de Madrid, Avda de la Universidad 30, E-28911, Leganés, Spain
{dds,dproserp,amarin,florina}@it.uc3m.es
[2] Fraunhofer Institut FOKUS, Kaiserin-Augusta Allee 31, 10589 Berlin, Germany
peter.weik@fokus.fraunhofer.de

Abstract. One of the most critical tasks when accessing services through the IP Multimedia Subsystem is the registration process. The process involves two registrations, the first with the access network, the second with IMS. This leads to an overhead authentication that introduces a big delay. This article proposes an improvement for IMS registration protocol able to relate IMS registration to an access network registration by cryptographically binding both of them. This approach provides a general solution, saves time during registration and avoids several attacks.

1 Introduction

IP Multimedia Subsystem (IMS) is an approach for specifying the evolution of circuit switched to packet switched networks with an special focus on fixed-mobile convergence. IMS services can be accessed independently from any access network as fixed networks, GPRS, UMTS, LTE, WIMAX and WiFi. IMS might cooperate with access network providers, for instance, in authentication duties. Future network scenarios present a single core network (IMS) that handles requests from clients connecting through access networks administrated by other companies. In such scenarios a user might spontaneously perform a vertical handover to increase bandwidth triggered by an application while others might be connected to different services through different access network technologies. For instance, a user watching a movie through its last-mile high speed optical fiber can be reading emails at the same time in a PDA attached to a GPRS station; both services might be provided by the same IMS core network. These scenarios are appealing since subscribers can remain attached to a GPRS or UMTS network almost everywhere while they can connect to any available 802.11b/g/n or Wimax hotspot on demand. The process of connecting to IMS services starts with the Mobile Equipment (ME) acquiring connectivity through an access network. This process involves the execution of an authentication mechanism that typically engages ME and its home network in a challenge response message exchange. However, the IMS home network might not be involved in the authentication process, for instance, a friend can give us the L2 authentication key of his wireless router. Once the ME has Internet connection it must register with IMS by exchanging again challenge-response messages. As the

J. Wozniak et al. (Eds.): WMNC 2009, IFIP AICT 308, pp. 32–43, 2009.

reader might infer, this double authentication process leads to a very time-consuming overhead, specially if the ME connects from a visited IMS network. For example, 3GPP requires for WLAN clients to execute an L2 authentication mechanism to authenticate with access network and then to authenticate to IMS (SIP-Digest-AKA). Interworking have been widely studied and many solutions have been proposed in order to reduce registration time giving as a result solutions ranging from those specifying incremental changes for a specific access network technology, that can be considered closed solutions, to those providing general tunneled protocols able to carry any authentication mechanism, that might suffer from Man-In-The-Middle attacks (MITM) if are not well defined. To overcome the problem, this article presents a general registration protocol for IMS that accelerates the process, while prevents MITM attacks by cryptographically relating access network registration to IMS registration.

2 Authentication for Accessing IMS Services

This section summarizes current IMS interworking with access networks, analyzes its benefits and drawbacks and recapitulates requirements for a general authentication scenario for interworking with non cellular access networks.

2.1 Authentication in the IMS

IP Multimedia Subsystem provides a control plane using Call Session Control Function (CSCF) servers by means of the Session Initiation Protocol (SIP) [1]. Subscriber data is managed by the Home Subscriber Server (HSS) and the Authentication Center (AuC). IMS defines the following types of CSCF servers. A proxy-CSCF (P-CSCF), the first hop in a visited network, that redirects SIP messages from ME to ME's home network. It also establishes an IPSEC security association with the ME. The confidentiality and integrity keys, C_K and I_K respectively, are derived as a result of the authentication performed with the HSS and conveyed to the P-CSCF using signaling. The I-CSCF, is an interrogating-CSCF located at home network that locates a server able to manage subscriber originated SIP messages. Finally, the **S-CSCF**, a serving-CSCF, authenticates subscribers retrieving authentication vectors from the HSS.

IMS authentication is based on HTTP Digest Authentication [2], using AKAv1-MD5 [3] as algorithm, which requires exchanging four messages (2 Round Trip Times-RTT) between the subscriber, at the visited network, and the subscriber's home network. IMS authentication leans on an UICC (Universal Integrated Circuit), a smart card located at ME, that contains an ISIM application (virtual subscriber module) which shares a long term secret (K_I) with the HSS. The IMS registration protocol works as follows (see also Fig. 1):

In the step 1, the ME is registered with the access network and has discovered a P-CSCF. In step 2, the ME uses the UICC to obtain subscriber information as the registration URI (to locate home network), the public/private identity and the Contact Address to build a SIP REGISTER message. Moreover, the ME includes a Security-Client header indicating which IPSEC algorithms supports. In step 3, the ME sends the aforementioned REGISTER message to the P-CSCF which inserts a P-Visited-Network

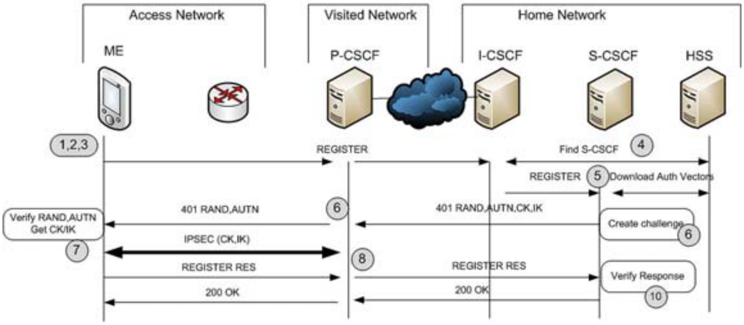

Fig. 1. Message exchange for a successful IMS registration

identifier in the REGISTER message. The P-CSCF reads and removes the Security-Client header and redirects the REGISTER message to the discovered I-CSCF (home network). The I-CSCF locates an appropriate S-CSCF to handle ME's messages by sending, in step 4, a Diameter User-Authentication Request (UAR) to the HSS. The REGISTER message reaches the S-CSCF at step 5. The S-CSCF downloads authentication vectors for the subscriber from the HSS. Those vectors are quintuplets containing parameters for authentication and key derivation using AKA [3] as: a random challenge (RAND), an authentication token (AUTN), the expected ME response (XRES), an integrity key (I_K) and a confidentiality key (C_K). AUTN is derived by the HSS using the long-term secret it shares with the ME (K_I) and a sequence number (SQN). The step 5 finish with the S-CSCF building a 401 Unauthorized message adding a WWW-Authenticate header containing AUTN and RAND. The S-CSCF includes also C_K and I_K in the message to be consumed by P-CSCF. Finally, the S-CSCF sends this message back to the ME. In step 6, the 401 Unauthorized message reaches the P-CSCF at visited network. The P-CSCF extracts and removes C_K and I_K from the message (the ME can derive C_K and I_K from AUTN and RAND using the UICC) and adds a Security-Server header selecting one IPSEC algorithm from those proposed by the client in step 2.

In step 7, the ME receives the 401 Unauthorized message and uses the UICC to calculate a response to the challenge (RES), C_K and I_K from AUTN and RAND. Then the ME establishes a security association with P-CSCF using C_K/I_K and composes a new REGISTER message containing RES and a Security-Verify header. Then it forwards the message to the P-CSCF over the brand new IPSEC security association. The P-CSCF, upon the reception of the message over a protected channel (C_K and I_K), implicitly authenticates the ME (step 8). Then, it redirects the message to the I-CSCF. The message is forwarded to the S-CSCF in step 9. Finally, in step 10, the S-CSCF receives the REGISTER message and checks if RES matches XRES to legitimate the subscriber. If the user is successfully authenticated, the S-CSCF builds a 200 OK message and sends it back to the ME finishing the IMS registration process.

2.2 Authentication in Access Networks

Cellular access networks, as UMTS, provide good coverage almost everywhere but data rates are far from being appropriate for several applications. As a result, interworking with other access technologies providing higher bandwidths is appealing: enables on demand or opportunistic vertical handovers when consuming IMS services. Authentication in 3G networks uses a secret stored in a smart card (UICC) to perform authentication and key derivation (AKA). The HSS also vouches for identities, being responsible of challenging a supplicant, verifying supplicant responses and deriving keys to protect radio channel. The virtual subscriber module handling the long term secret used for 3G authentication (K_U) is called USIM and is collocated at the UICC together with ISIM (K_I). Thus, authentication mechanisms for Packet Switched domain (3G) and IMS are independent so a double authentication is performed.

The authentication process in other access networks varies with the technology. For instance, IEEE 802.11 relies on L2 access control and security mechanisms specified by IEEE 802.11-1999 Part 11 that specifies L2 encryption, IEEE 802.1X describes a Network Access Control that uses Extensible Authentication Protocol (EAP), and IEEE 802.11i which supersedes WEP and WPA. Besides, WiFi public services authentication is often performed against a web site leaving L2 unprotected. Others, as Long Term Evolution provides security features in MAC level. 3GPP enforces some requirements for 3G interworking with other access networks: first, the UMTS security architecture must not be compromised and second, authentication must be mutual, based on a challenge-response mechanism using the long term secret stored in UICC and must result in a key derivation. These requirements reduces the amount of authentication algorithms that can be used during the authentication with access networks, in practise, lead to the adoption of AKA.

There are several drawbacks in this interworking scenario. Regarding the time spent during authentication, AKA requires 2 RTTs to convey the challenge to the ME and to receive the response, thus, when combined with IMS authentication yields to 4 RTTs. Moreover, the adoption of AKA requires implementing EAP-AKA for every access network technology (even in L2) in contrast with the benefits, for instance, scalability, cost-effectiveness and early adoption of new technologies, of using protocols above network layer, as PANA [4] that carries EAP payloads.

2.3 General Tunneled Authentication Mechanisms

UMTS and IMS authentication protocols are independent from each other and their subscriber modules, USIM and ISIM respectively, handle different key material. However this key material might be reused for access network authentication preventing the UICC from implementing a subscriber module for any upcoming technology. This obvious simplification introduces a feasible MITM attack since the algorithm has no way to know the purpose of the authentication, for instance, a MITM can use victim's network authentication messages to impersonate the subscriber obtaining access to the same or other network expecting those credentials. This attack can be prevented only if the authentication mechanism results in a key derivation and the key is used to protect the channel between supplicant (ME) and authenticator (typically the Network Authentication Service - NAS).

There are many works proposing general tunneled authentication mechanisms that enable carrying EAP payloads over other protocols. The idea behind is to reuse legacy authentication protocols for other purposes creating a tunnel that authenticates the NAS before starting the inner authentication mechanism. Once the NAS is correctly authenticated, it will forward authentication messages (inner protocol) to a back-end authentication service (typically the HSS). In this way, an authentication protocol inside the tunnel can be reused in a secure fashion since it is executed over a tunnel between the client and the NAS. Moreover, this tunneled protocols help to alleviate the problem of having implemented authentication protocols in L2 by providing an alternative transport over a higher protocol. Nevertheless, the feasibility of aforementioned MITM attack is already present. The reason is that this kind of tunnel protocols require to distribute credentials to every NAS, since the NAS should be authenticated. The problem is explained in [5] and [6] and appears when an authentication protocol is designed as the combination of two protocols: an outer protocol and an inner protocol. The outer protocol, for instance TLS [7], is used to protect the exchange of messages of the inner protocol. The inner protocol is used to authenticate the user to the network and the outer to authenticate the network to the user. Among the protocols affected by this attack we can find PEAP, EAP-TTLS, PIC and PANA over TLS [8]. The problem appears under any of the following conditions. 1) The inner protocol can be used in other environments. It happens when the inner protocol has no way to know if it is used inside a tunnel or not. 2) The client fails to verify the server certificate in the outer protocol. This might be frequent when connecting to access networks since the ME lacks of connection to Internet to download Certificate Revocation Lists (CRLs) or any other information necessary to verify NAS certificate. Besides, despite this is an unacceptable error from client side, the network must provide mechanisms to overcome the fact that a single client error can compromise security (specially when non professional users are involved).

The attack works as follows: the MITM waits until a legitimate device (ME) starts an untunneled legacy remote authentication protocol. Then, the MITM starts a tunnel with an authentication agent (access network) and starts sending legitimate user's authentication messages over the tunnel until the legitimate client is successfully authenticated. Then, the MITM derives keys to protect the channel from the outer tunnel keys stealing service to the legitimate client. To overcome this attack there are two simple solutions. In the first, the inner protocol must provide not only authentication but also must result in a key derivation. Those keys should be used to protect a channel between the client and the server. Thus, there is an implicit authentication since only the client knows those keys. However, it can be solved if the outer tunnel keys are derived from the long-term secret used in the inner protocol or both inner protocol and outer tunnel are somehow related.

2.4 Security Analysis of the IMS Registration

A new registration protocol must provide, at least, the same degree of security as the previous protocol. For that reason we perform a basic security analysis of the standard IMS registration using BAN logic [9] to identify the believes and how the different entities authenticate each other (implicitly or explicitly). The initial conditions are: the ME has connection to Internet through an access network, L2 is protected and the ME shares a long term secret called K_I with the HSS.

$$\mathrm{ME} \Leftrightarrow_{k} \mathrm{HSS}$$

Step 3 : The P-CSCF includes a P-Visited-Network in REGISTER asserting its identity to subscriber's home network. The REGISTER message is transmitted over a security interface among providers (Za).

S-CSCF believes (P-CSCF said REGISTER)

Step 6 : The P-CSCF receives I_K and C_K from S-CSCF over secured inter-provider network.

P-CSCF beleives (S-CSCF said I_K,C_K)

Step 7 (A) : The ME is able to extract I_K, C_K, AUTN and RAND from WWW-Authenticate, so it is able to **authenticate the home network**.

Since ME $\Leftrightarrow_k$ HSS and
ME sees $\{I_K, C_K, AUTN, RAND\}$ from $\{I_K, C_K, AUTN, RAND\}_K$
then ME beleives (S-CSCF said $\{I_K, C_K, AUTN, RAND\}_K$).

Step 7 (B) : The ME believes that P-CSCF is trusted since its home network accepts it as valid. Step 7 (C) : The ME creates a security association with an endpoint X using I_K and C_K. Since C_K and I_K are provided by ME's home network to a trusted P-CSCF, the ME is sure the endpoint X is the P-CSCF.

Since ME believes (ME $\Leftrightarrow_{C_K, I_K}$ P-CSCF) and
ME sees {IPSEC-Payload}$_{C_K, I_K}$
then ME believes (P-CSCF said IPSEC-Payload).

Step 8: The P-CSCF receives the REGISTER message with a response to the challenge over the security association so ME is implicitly authenticated by P-CSCF.

Since ME believes (ME $\Leftrightarrow_{C_K, I_K}$ P-CSCF) and P-CSCF sees $\{REGISTER\}_{C_K, I_K}$
then P-CSCF believes (ME said REGISTER).

Step 10: The S-CSCF checks the response message from the ME by comparing RES with XRES. If both are equal, S-CSCF **authenticates the ME**. The security analysis is the same as for Step 7 (A).

3 Registration for Secure Interworking with Access Networks

The objectives of the proposed registration framework are to reduce the registration time, to provide a general authentication framework for any upcoming technology, to prevent attacks, to fulfill 3GPP requirements, and to maintain backwards compatibility. For that reason, the requirements for the registration protocol are: 1) The access network registration must be performed over any layer, thus the authentication must be based on an EAP method suitable to be used over L2 or an upper level (PANA) EAP carrier. 2) The ME must be able to both authenticate the NAS and cryptographically prove access network registration to IMS. Moreover, L2 must be protected. For that reason, the EAP method must securely derive keys (EAP-TLS) and a cryptographic proof of the message exchange (TLS Exporter[10]). 3) The IMS registration should be cryptographically related to access network registration. 4) The security association between ME and P-CSCF should be protected with a key derived from the long term secret K_I and the access network registration proof. The scenarios are shown in Fig. 2. In the first

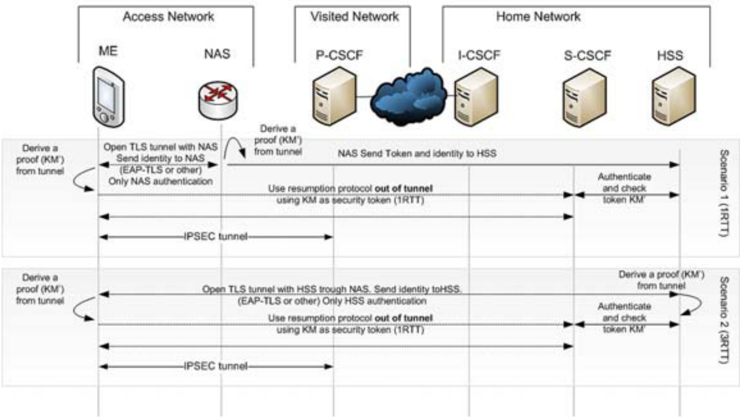
Access Network
Visited Network
Home Network
ME
NAS
P-CSCF
I-CSCF
S-CSCF
HSS
Derive a proof (KM') from tunnel
Open TLS tunnel with NAS Send identity to NAS (EAP-TLS or other) Only NAS authentication
Derive a proof (KM') from tunnel
NAS Send Token and identity to HSS
Authenticate and check token KM'
Use resumption protocol **out of tunnel** using KM as security token (1RTT)
IPSEC tunnel
Scenario 1 (1RTT)
Derive a proof (KM') from tunnel
Open TLS tunnel with HSS trough NAS. Send identity toHSS. (EAP-TLS or other) Only HSS authentication
Derive a proof (KM') from tunnel
Authenticate and check token KM'
Use resumption protocol **out of tunnel** using KM as security token (1RTT)
IPSEC tunnel
Scenario 2 (3RTT)

Fig. 2. Scenarios for resumption protocol with cryptographic relation to access network tunnel

scenario, the ME opens a tunnel with NAS using EAP-TLS over L2 or PANA. The ME provides an identifier to the NAS so the NAS can resolve ME's home network address. The NAS extracts key material from the tunnel using TLS exporter. It derives two proofs (P_N and P_I) from the TLS key material using a Pseudo Random Function (PRF) over the result of concatenating the master key with two different texts. The ME extracts key material and derives the same proofs. The ME then starts the IMS authentication process. It includes P_N as a token in a SIP REGISTER message and protects message integrity with a signature (that signature can be checked by the HSS). Simultaneously, the NAS sends P_N and P_I to the HSS using Diameter. The signature is used to authenticate the ME and P_N is used by the HSS to relate access network to IMS network. Finally, the HSS provides IPSEC keys for confidentiality and integrity. Those keys are derived as follows $C'_K = PRF(C_K|P_I)$ and $I'_K = PRF(I_K|P_I)$ relating both authentication processes to prevent MITM attacks. In this way, the HSS can explicitly authenticate the ME (signature), the ME can implicitly authenticate the NAS and the NAS can implicitly authenticate the ME. This process saves 3 RTT without compromising security and avoiding MITM attacks. In the second scenario, the EAP-TLS tunnel is opened directly with the HSS saving only 1 RTT.

We rely on an asymmetric ephemeral key that must be registered by the ME before being used. This key should be able to generate signatures. Providers might enforce minimum length and a validity period policies. The key, called R_k (resumption key), should be stored in the HSS (with a key index) together with the token provided by the access network. Moreover, the token might be used to resume a previous IMS session in other contexts.

3.1 Protocol Definition and Security Analysis

In this section we describe the proposed registration protocol in detail. The description assumes that the user has already derived a public/private key pair and registered the public key (R_k) under his profile at HSS. The ME opens a EAP-TLS tunnel with the

NAS (1^{st} scenario) using PANA or a L2 protocol. Once both the HSS and the ME have available the cryptographic proofs P_N and P_I (step 1), the ME registers with IMS as follows (see Fig.3).

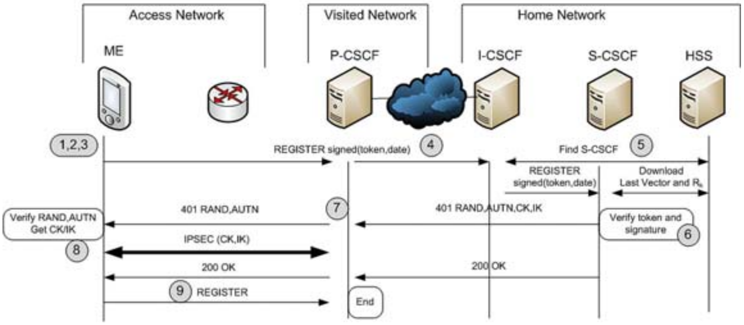

Fig. 3. Message exchange for a successful IMS registration resumption

In step 2, the ME builds a REGISTER message, as in standard IMS registration (described in Sect. 2.1) except for the inclusion of an *Authorization* header. Then, in step 3, the ME includes a **nonce** field as part of the *Authorization* header. This field contains a token obtained from a tunnel with the NAS (P_N), that will be used to relate both registrations. The ME also adds an *auth-param* to the *Authorization* header with the text *"resume@idx"*, indicating the index under R_k is registered. Finally, the ME generates a S/MIME body including: information from headers as explained in Authenticated Identity Body Format [11], the *Authorization* and Security-Client headers and a signature generated with R_k.

The ME sends the REGISTER message outside the tunnel to the P-CSCF which inserts a P-Visited-Network identifier. The message is forwarded to the I-CSCF at ME's home network (step 4). The I-CSCF finds a S-CSCF (step 5). The REGISTER message reaches the S-CSCF in step 6. Then, the S-CSCF extracts **key index** and **nonce** parameters from REGISTER headers, contacts the HSS to download the tokens (P_n and P_I), R_k and new authentication vectors. The S-CSCF builds a 401 Unauthorized message containing a WWW-Authenticate header with a nonce (AUTN—RAND) obtained from a **new authentication vector**. The S-CSCF checks if the nonce contains the same P_N received from the NAS and the signature. If both the signature and the token (P_N) are valid, the S-CSCF **authenticates the subsriber**. To inform the ME about the successful authentication, the S-CSCF includes an *auth-param* parameter in the WWW-Authenticate header of the 401 message with the text *"resume@idx"*. Moreover, the S-CSCF derives two keys for integrity and confidentiality, $I'_K = PRF(I_K|P_I)$ and $C'_K = PRF(C_K|P_I)$ and include them in the message for the P-CSCF. The S-CSCF sends it to the ME through the I-CSCF and P-CSCF. Then it builds a 200 OK message that will be sent immediately after the 401 Unauthorized message. Otherwise, if the S-CSCF either does not support this registration protocol or the ME can not be authenticated, it sends a 401 message to the ME without modifying the WWW-Authenticate header (as standard registration).

In step 7, the P-CSCF extracts and removes C'_K and I'_K from the 401 Unauthorized message and adds a Security-Server header selecting an algorithm for IPSEC. In step 8, the ME extracts AUTN, RAND, I_K and C_K from the WWW-Authenticate header **authenticating explicitly the home network**. If the WWW-Authenticate header contains the *auth-param* parameter, the ME derives $I'_K = PRF(I_K|P_I)$ and $C'_K = PRF(C_K|P_I)$. Then it establishes a security association with P-CSCF and waits until a 200 OK message is received. Otherwise, it behaves like standard registration deriving a response to the challenge (RES) and composing a new REGISTER with the response. Step 9: if the registration protocol was accepted by the S-CSCF (the message contains an auth-param) the ME creates a REGISTER message containing only a Security-Verify header. This message must be consumed by the P-CSCF at visited network thus, the **TO** header points to the P-CSCF. The ME sends this REGISTER message to the address of P-CSCF over the brand new security association finishing the registration.

3.2 Security Considerations

In this section we analyze the proposed protocol showing that is as secure as standard protocol. Initial conditions: the ME and the HSS shares a long term secret called K_I, an ephemeral resumption key called R_k and two security tokens (P_I and P_N):

$$\text{ME} \Leftrightarrow_{K_I,R_k,P_I,P_N} \text{HSS}$$
$$\text{HSS believes (ME has jurisdiction over } R_k)$$

Step 4 : The P-CSCF includes a P-Visited-Network in REGISTER asserting its identity to subscriber's home network. The REGISTER message is transmitted over a security interface among providers. (equivalent to standard registration, step-3).

Step 6: The S-CSCF receives the REGISTER message from the ME, it downloads the R_k,P_I,P_N and a new authentication vector. It first checks the date and P_N contained in the message against the information downloaded from the HSS. Then it checks the signature against R_k. If the signature is valid and the date and P_N are valid, the S-CSCF authenticates the subscriber.

HSS believes (ME has jurisdiction over R_k) and
S-CSCF believes (ME believes nonce[1])
then S-CSCF believes nonce.

S-CSCF believes (ME said nonce) and
S-CSCF believes nonce is fresh
then S-CSCF believes (ME believes nonce).

Step 7 : The P-CSCF receives I'_K and C'_K from S-CSCF over secured inter-provider network. (equivalent to standard registration, step-6). Step 8 (A) : The ME is able to extract I'_K, C'_K from AUTN and RAND, so it is able to **authenticate the home network**. (equivalent to standard registration, step-7A).

Step 8 (B) : The ME believes that P-CSCF is trusted since its home network accepts it as valid.Step 8 (C) : The ME creates a security association with an endpoint X using I'_K and C'_K. Since C'_K and I'_K are provided by ME's home network to a trusted P-CSCF, the ME is sure the endpoint X is the P-CSCF. (equivalent to standard registration, step-7C).

[1] This nonce is the base64 representation of the security token.

C'_K and I'_K depends on P_I; P_I was derived from the tunnel with the NAS, thus there is no MITM.

Step 9: The P-CSCF receives the REGISTER message with a Server-Verify header over the security association so ME is implicitly authenticated by P-CSCF (equivalent to standard registration, step-8). Table 1 summarizes both protocols authentication processes showing which entities are explicitly or implicitly authenticated.

Table 1. Authentication among entities during registration for both protocols

Authentication	Standard	Proposed
Home network authenticates visited network (federation)	step 3	step 4
Visited network authenticates home network (federation)	step 6	step 7
Home network authenticates ME (explicit)	step 10	step 6
ME authenticates home network (explicit)	step 7A	step 8A
ME authenticates visited network (implicit)	step 7b-7C	step 8B-8C
Visited network authenticates ME (implicit)	step 8	step 9

4 Related Work

[12] proposes a solution for secure authentication in a heterogeneous wireless access scenario. This solution requires moving part of the P-CSCF functionality (including security association) to the access network. This WLAN P-CSCF redirects ME's REGISTER messages to the visited network inserting a header that indicates the type of authentication demanded by the ME (WLAN and IMS or WLAN only). This header is not protected thus it can compromise security. Moreover, the home network must allow its key material to be populated to access networks thus requires strong trust relations between IMS operators and access networks. Our proposal does not modify IMS architecture. Moreover we provide an IPSEC association protected with keys derived from two authentication processes avoiding masquerades even from unknown access networks.

In [13] the authors propose a one pass authentication procedure to obtain access to IMS services over GPRS access networks. The author proposes a modification to SGSN that adds the IMSI (associated with a PDP context) to any register message so the S-CSCF can check if the IMPI matches the corresponding IMSI authenticating the user. This solution can not be considered general. Besides, the authentication in IMS is performed without cryptography thus any user might impersonate other just by manipulating the IMSI. Other solutions as [14], propose to move the authentication to layer two using 802.1x with EAP-AKA, thus removing authentication at service level. This kind of solutions are not independent from the specific access technology so requires defining an specific procedure for any incoming technology. Our solution is a general approach to the interworking problem. It can be used with any upcoming access technology since it can be used either over L2 or PANA. [15] proposes a make-before-break handover scheme under IMS that defines a set of new SIP headers to negotiate a security association with the new visited access network speeding up the registration process. The modifications we propose are compatible with this solution also. In [16], the registration is accelerated by reducing the amount of messages exchanged between the I-CSCF and the HSS to find an appropriate S-CSCF. Those improvements are also compatible with our solution.

5 Conclusions

This article describes a registration improvement for IMS that allows using a security token to relate network access registration with IMS registration (or to resume an older IMS registration). The proposed protocol can be used by any upcoming access network technology since the access network registration can be done over L2 or PANA. Moreover, it avoids several attacks since UICC credentials are not exposed during access network registration but the entire registration process (access network and IMS) depends on the successful registration with IMS. We achieve this goal by cryptographically relating IMS registration to access network registration in such a way that only the owner of the UICC will be able to derive the final IPSEC keys if knows P_I. We analyzed the security of our proposed registration protocol and compared to the standard IMS registration security showing that both of them provide the same degree of security. Moreover, we save up to 3 round trip times during the registration.

References

1. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: Sip: Session initiation protocol. Technical Report RFC3261, IETF (2002)
2. Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., Stewart, L.: Http authentication: Basic and digest access authentication. Technical Report RFC2617, IETF (1999), http://www.ietf.org/rfc/rfc2617.txt
3. Technical report, 3GPP, Third Generation Partnership Project, Technical Specification Group Services and Systems Aspects, 3G Security, Security Architecture, Technical Specification 3G TS 33.102, V3.7.0 (2000)
4. Parthasarathy, M., et al.: Protocol for Carrying Authentication and Network Access (PANA) (RFC 5191 - 2008), PANA Threat Analysis and Security Requirements (RFC 4016 - 2005), PANA Requirements (RFC 4058 - 2005)
5. Puthenkulam, J., et al.: The Compound Authentication Binding Problem. Technical report, IETF (2003)
6. Asokan, N., Niemi, V., Nyberg, K.: Man-in-the-middle in tunneled authentication protocols. Technical report. In: 11th Security Protocols Workshop (2002)
7. Dierks, T., Allen, C.: The transport layer security (TLS) version 1.0. Technical Report RFC2246, IETF (1999), http://www.ietf.org/rfc/rfc2246.txt
8. Ohba, Y., Baba, S.: Pana over tls. Technical report, IETF (2002)
9. Burrows, M., Abadi, M., Needham, R.: A logic of authentication. ACM Transactions on Computer Systems 8, 18–36 (1990)
10. Rescorla, E.: Keying material exporters for transport layer security (tls). Technical Report draft-ietf-tls-extractor-05.txt, IETF (2009), http://tools.ietf.org/html/draft-ietf-tls-extractor-05
11. Peterson, J.: Session initiation protocol (sip) authenticated identity body (aib) format. Technical Report RFC3893, IETF (2004), http://www.ietf.org/rfc/rfc3893.txt

12. Veltri, L., Salsano, S., Martiniello, G.: Wireless lan-3g integration: Unified mechanisms for secure authentication based on sip. In: IEEE International Conference on Communications, 2006. ICC 2006, vol. 5, pp. 2219–2224 (2006)
13. Lin, Y.B., Chang, M.F., Hsu, M.T., Wu, L.Y.: One-pass gprs and ims authentication procedure for umts. IEEE Journal on Selected Areas in Communications 23, 1233–1239 (2005)
14. Celentano, D., Fresa, A., Longer, M., Robustelli, A.: Improved authentication for ims registration in 3g/wlan interworking. In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007, pp. 1–5 (2007)
15. Lee, H., Moon, B., Aghvami, A.: Enhanced sip for reducing ims delay under wifi-to-umts handover scenario. In: Next Generation Mobile Applications, Services and Technologies. NGMAST 2008, pp. 640–645 (2008)
16. Farahbakhsh, R., Varposhti, M., Movahhedinia, N.: Transmission delay reduction in ims by re-registration procedure modification. In: Next Generation Mobile Applications, Services and Technologies. NGMAST 2008, pp. 142–146 (2008)