End-to-middle-to-end solution for IMS media plane security

Jose Oscar Fajardo[1,*], Fidel Liberal[1], Fudong Li[2], Nathan Clarke[2] and Is-Haka Mkwawa[3]

[1] Dpto. Ingeniería de Comunicaciones, University of the Basque Country (UPV/EHU), ETSI Bilbao, Almda Urquijo s/n, 48013 Bilbao, Spain

[2]Centre for Security, Communications and Network Research (CSCAN), Plymouth University, Portland Square, Plymouth, PL4 8AA, United Kingdom

[3]School of Computing and Mathematics, Plymouth University, Smeaton Building, Plymouth, United Kingdom

E-mail: {joseoscar.fajardo; fidel.liberal}@ehu.es, {fudong.li; N.Clarke; is-haka.mkwawa}@plymouth.ac.uk

* Corresponding author

Tel.: +34-946017202; Fax: +34-946014259

Abstract IP Multimedia Subsystem (IMS) is becoming the prevailing candidate for managing future mobile multimedia communications, including critical communications such as public safety, emergency professionals and corporate networks. IMS security and privacy has gained much attention in the few last years. The review of recent IMS security activities stresses the inclusion of intermediate nodes in the media path of secured communications as an open issue. This paper presents an end-to-middle-to-end solution which enables the usage of IMS media plane elements such as recorders, transcoders and novel cross-ciphering functions in a secure way. The proposed solution, which is fully compliant with IMS, includes the network architecture, the signaling plane for session signaling and key management, and the media-plane security characteristics. Experimental results demonstrate that the proposed solution can provide media interoperability (both transcoding and cross-ciphering) with a cost of 17% overhead to a standard IMS call setup in the signaling plane.

Keywords: IMS, media plane security, cross-ciphering, security resource function.

1 Introduction

The forthcoming deployment of 4th Generation (4G) networks is revolutionizing the way that mobile communication networks will be provisioned, moving from the traditional circuit-switched approach to an all-IP based communication environment. Currently, Long Term Evolution (LTE) is becoming the prevalent network technology which is selected by mobile network operators worldwide for the implementation of future mobile communications [31]. LTE was introduced by the 3rd Generation Partnership Project (3GPP) in its Release 8 and provides evolved capabilities in terms of network performance, mobility management and security mechanisms. However, LTE does not intrinsically comprise the use of any communication establishment protocol to process calls (e.g. call setups), resulting it has to rely upon other protocols to manage the call establishment in the signaling plane. Otherwise, it would only provide a seamless mobile IP connectivity to end users.

Although any Over-The-Top (OTT) solution may enable IP-based communications over LTE, IP Multimedia Subsystem (IMS) has become the prevailing candidate for 4G commercial-grade network-operated multimedia services [23]. IMS defines a whole session management layer over heterogeneous networks, including Session Initiation Protocol (SIP)-based procedures for the end-to-end negotiation of the session characteristics [1]. Regardless of IMS technology independence, the end-to-end negotiated parameters may be propagated to the underlying network infrastructures in order to make use of their capabilities such as security or Quality of Service (QoS). This is the case of LTE, which defines the proper management of IMS traffic over specific Evolved Packet System (EPS) Bearers. IMS understands LTE as an IP-enabled access network and is able to make use of LTE enhanced transport capabilities in a per-session basis.

IMS security and privacy has been a challenging topic and has received a significant amount of attention during the last few years [32, 22]. Although IMS benefits from specific security and privacy mechanisms in the LTE air interface and core infrastructure [16], additional IMS-level mechanisms are required especially in multi-domain communications. In order to secure an IMS enabled communication channel, two areas must be analyzed: the signaling plane and the media plane.

1.1 IMS signaling plane security

For the signaling plane security, the 3GPP standardized IMS security is governed by [2] and [4] which define the mechanisms to protect the SIP messages between the endpoints of both inter and intra

domain communications in terms of confidentiality, integrity and authentication. Since the early 3GPP Release 5, both documents are regularly updated with enhanced security mechanisms. In order to ensure the IMS signaling plane security, IMS Authentication and Key Agreement (AKA) is used for mutual authentication and for agreeing confidentiality and integrity keys between the User Equipment (UE) and the Proxy Call Session Control Function (P-CSCF). The security of SIP messages is then implemented based on Transport Layer Security (TLS) with the agreed keys.

The security of the IMS signaling plane is critical because it is utilized not only to avoid impersonation and Denial of Service (DoS) attacks, but also to protect the privacy of the communication in terms of participating identities, network addresses, etc. Furthermore, recent legislations in Next Generation (NG) emergency communications (e.g. the U.S. NG 911, the European NG112 and the Australian national emergency warning system (NEWS)) enforce the automatic location of callers within the SIP header fields [28, 7]. If the SIP message is not secured, the caller's privacy will be compromised. Therefore, the security of the IMS signaling plane becomes even more critical than ever.

The security of the SIP signaling has been thoroughly analyzed by the research community as a major concern of IMS infrastructures. Although extensive surveys analyze the vulnerabilities of SIP and general Voice over IP (VoIP) solutions [22, 18], only those that apply to IMS infrastructures are considered in this paper. [20] provided a revision of the security concerns within an administrative IMS domain from the perspective of both the network providers and the network users. The typical DoS problem from the perspective of IMS emergency communications is analyzed by [27]. In addition, [21] analyzes the IMS DoS problem in 3rd Generation (3G) Universal Mobile Telecommunication System (UMTS). [13] differentiates between the 3GPP intra and inter domain security architectures and categorizes the possible time-dependent and time-independent attacks to the IMS signaling plane. Besides this categorization, [32] also discriminates internal and external attacks and the effects of attacks in terms of confidentiality, integrity, authentication and service availability. Based on these categories, [32] provides a thorough evaluation of the robustness of the IMS architecture proposed by the 3GPP as well as considering a series of state-of-the-art research proposals. Hence, these works demonstrate that the standardized solution based on IMS AKA and TLS provides the adequate protection against external attacks, although several vulnerabilities are identified especially during the initial user registration process.

1.2 IMS media plane security

Regarding the media plane security, it is regulated by [5] which was introduced in the Release 9 by the 3GPP, much more recently than its signaling counterpart. Nonetheless, it is the key document that states how multimedia IP flows should be securely protected in various possible network scenarios. In general, the IMS media flows are protected by the Secure Real-time Transport Protocol (SRTP) (which is a media authenticated encryption method) and a security key exchange protocol. From the categorization introduced in [6] the following media plane security situations shall be considered (as illustrated in Fig. 1):

- End-to-end (e2e) security makes use of the security characteristics (type of cryptographic mechanisms, including the method to share the ciphering keys) negotiated by the endpoints of the communication to protect the media plane packets.
- End-to-access-edge (e2ae) security enforces additional security parameters in the transit of media packets from the endpoint to an IMS access-edge element; this way, the media plane can be protected through non-reliable access networks while the rest of the media path which is within the core IMS media network may be kept unencrypted. [21] analyzes the architectural problems of UMTS and possible signaling attacks on the UMTS core. Concerning more recent 4G networks, as stated in [16], the need of an e2ae solution over LTE access is not critical since LTE provides strong access security both in the radio and core segments.
- End-to-middle (e2m) security is conceived to support the transit from IMS networks to legacy networks, where specific security mechanisms shall be supported; in this case, the protection is carried out between an IP endpoint to an IMS Media Gateway which also supports the legacy network.
- End-to-middle-to-end (e2m2e) security is aimed at allowing trustworthy network nodes to access the plaintext media of a secured communication, which serves two main purposes: interoperability and lawful interception. When endpoints utilize incompatible security mechanisms, e2m2e can provide the interoperability for these endpoints without compromising the media plane security. Also, this approach can support lawful interception if required, as the encrypted data can go through a middle point (e.g. a monitor of a law enforcement agency) even though endpoints are qualified for an e2e security communication.

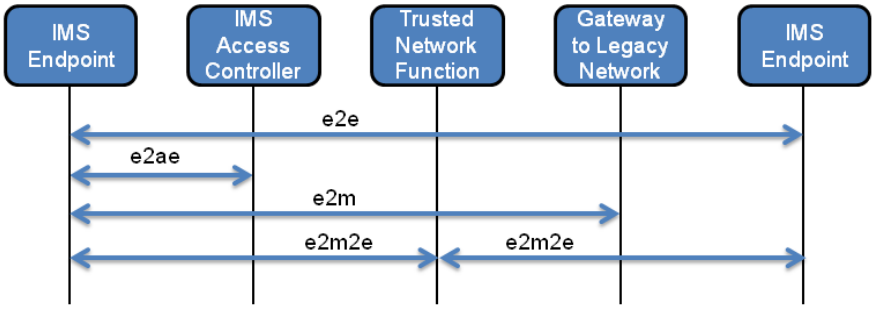

Fig. 1 Media-plane security alternatives

While the first three situations have been endowed with specific technical solutions to support the required functionalities [1, 5], the e2m2e approach is not yet standardized. Therefore, technical solutions will be required where IMS/LTE encrypted media would build daily operations not only for regular users but also in areas of online commerce [24], enterprise communications, public safety and emergency operations between different professional organizations [15].

To date, the media plane security has received far less attention from the scientific community in comparison with the amount effort given in the signaling plane. [22] evaluates a set of 245 research publications related to VoIP security, from which less than 10 references were devoted specifically to media plane security solutions. Nonetheless, these media plane security related studies were merely focused on the performance of different key exchange protocols.

From the perspective of the e2m2e proposal, the involvement of IMS resource functions requires that the IMS control entities include a number of network-operated intermediate entities in the media path. [19] analyzes the limited capabilities for legal interception in pure SIP networks considering the end-to-end key negotiation. [17] suggests that IMS control nodes may act as a man-in-the-middle element if the keying information is exchanged at the SIP signaling level. This way, a trusted node may have the access to the clear-text media for cross-ciphering, lawful recording or transcoding purposes.

1.3 Scope of the paper

As demonstrated in the last section, none of the research works clearly identified how security network functions can be integrated into the overall IMS framework despite some consideration was given to capture the session keying information and derive it to a trusted node. Therefore, this paper proposes a novel solution that makes the use of a trusted network resource node which has the media cross-

ciphering ability to secure communications even though endpoints are not compatible with each other. This proposal is originally considered of utmost relevance in certain environments such as emergency communications between field professionals who belong to different administrative organizations. Additionally, the proposed architectural solution resembles the standardized IMS architecture for media transcoding functions.

In summary, this paper aims at defining a technical solution that covers all aspects related to the inclusion of an e2m2e element in the standardized IMS architecture, including the definition of the network architecture, the signaling plane for session signaling and key management, and the media-plane security characteristics. The proposed solution allows the use of media transcoding or recording functions in the media path and also enables the possibility to reassure secured communications with media cross-ciphering capabilities. Furthermore, the solution copes with the 3GPP standardized IMS architecture and procedures and thus it can be implemented over current IMS deployments.

The rest of the paper is structured as follows. Section 2 presents the overall network architecture and identifies the proposed functional entities. Section 3 provides the details of a novel IMS ciphering resource function. Detailed information about protocols, messages and data formats for the implementation of the system is described in section 4 while a performance evaluation of the proposal is presented in section 5. Finally, Section 6 presents the conclusions to the paper and highlight future works.

2 Network architecture for the media-plane e2m2e solution

The proposed e2m2e network solution is illustrated in Fig. 2. Firstly, a new Secure Multimedia Resource Function (SMRF) entity is defined as the main controller for the novel media plane security functions in the IMS signaling plane. The SMRF is introduced in the IMS infrastructure as an Application Sever (AS) and interfaces with the Serving-Call Session Control Function (S-CSCF) through the standard IMS Control Interface (ISC). The inclusion of this new SMRF AS in the signaling plane does not comprise any modification in the standardized IMS elements, and only the suitable configuration of the specific Trigger Point is required. When required by configuration, the core CSCF nodes insert the SMRF in the signaling path of the IMS communication which enables it to control the

SIP dialog and the negotiation of the session parameters on behalf of two resource function nodes: the Multimedia Resource Function (MRF) and a Security Resource Function (SecRF). The IMS standard MRF is responsible for the operations involving the processing of the media content, such as transcoding for reassuring compatibility between endpoints, recording for lawful interception or mixing media flows for group communications. Meanwhile, the SecRF is introduced as a new IMS functional entity which is specialized in implementing any required encryption/decryption operations at the media plane level. These two nodes are kept out of the SIP signaling path so they do not have direct access to users' information.

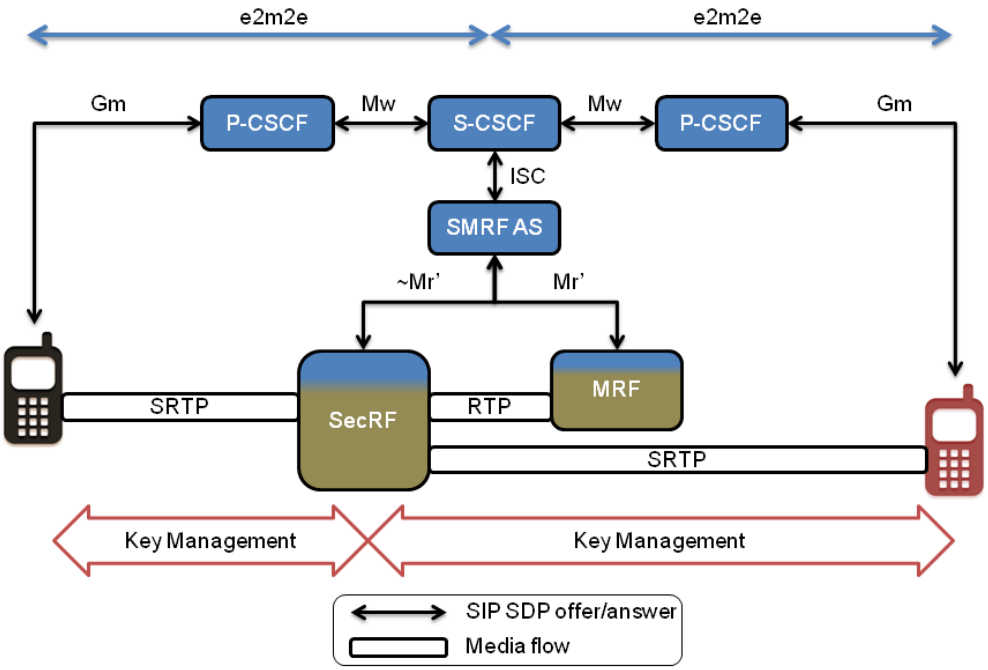

Fig. 2 Proposed network architecture for IMS e2m2e security

From the perspective of the end-to-end communication, the SMRF acts as a 3rd Party Call Controller (3PCC) [1, 3]. Thus, the SMRF is able to control and modify the SIP parameters negotiated by the endpoints as an authorized IMS control element with routing back-to-back user agent (B2BUA) functionalities. Since it is included in the SIP dialog, a unique SMRF AS is able to handle the media security capabilities of the different endpoint involved in the communication. As illustrated by Fig. 2, the SMRF also interfaces with the media plane resource function entities in order to capture/configure their media processing capabilities. Following the standardized MRF approach, this procedure is based on a new SIP dialog initiated by the SMRF to the required resource function [3]. Considering the media

plane elements, the SMRF acts as an initiating user agent and establishes independent SIP dialogs with each required resource function following the concepts of the standard Mr' interface.

It must be noted that the definition of the new SMRF AS element assures the compliance with the current IMS architecture. Yet, the proposed design is flexible enough in the sense that the SMRF functions may be integrated into existing IMS control elements. Currently, the S-CSCF is able to manage the inclusion of the MRF into the media plane. Followed by the same principle, the S-CSCF could be able to perform the proposed SMRF procedures in order to interface with both the SecRF and the MRF in future. Similarly, any 3PCC-like AS such as Multimedia Telephony (MMTel) AS or Service Centralization and Continuity (SCC) AS could also be implemented with these SMRF functions and the SMRF AS will not be required anymore.

According to the IMS standard specifications (Section 4.7 in [1]) the MRF is divided into two elements: a signaling-level controller and a media-level processor. Hence, the SecRF functional entity can also be split into two sub-functions: a SecRF Controller (SecRFC) and a SecRF Processor (SecRFP). The SecRFC is in charge of processing the SIP messages received by the SMRF while the SecRFP implements the specific operations related to the media packets. For simplicity, both functions are integrated into the SecRF node in Fig. 2. Also illustrated by Fig. 2 the SecRF element is able to manage three different SRTP flows, acting as an intermediate endpoint to the actual end users and a peer endpoint to the MRF. In order to enable this operation, the SMRF sends information about the end users' security characteristics negotiated at the IMS signaling plane to the SecRF. From this information, the SecRF is able to perform the key management procedures required by each endpoint. In comparison, the MRF entity is only able to access the plaintext media for various purposes (e.g. transcoding and/or legal interception) when the SMRF configures a media connection between the SecRF and the MRF. This connection may be a double media communication if the MRF needs to send back the media packets to the SecRF after processing them.

2.1 Session setup process: offering media capabilities

The session establishment procedure between two individual IMS endpoints (denoted by UE1 and UE2) follows the standard Session Description Protocol (SDP) offer-answer model [29]. Basically, the originating UE1 generates an SDP Offer with the supported/desired media parameter and includes this information in a SIP INVITE message to the destination UE2. When UE2 is compatible with UE1, it

selects a desired set of media parameters from the SDP offer and sends back an SDP Answer in a SIP 200 OK message; when UE2 is not compatible with UE1, it will reply with a SIP 606 Not Acceptable message and the SIP dialog will end.

In the context of the IMS call management, there are two main mechanisms to include additional session characteristics in the SDP negotiation [1, 3]:

- In the reactive approach, the IMS control entity examines if the answer of UE2 indicates the incompatibility in the supported media formats. In that case, the IMS control node requests the resource function to allocate resources for the session and generates a new SDP Offer to UE2 with the additional capabilities.
- In the proactive approach, the IMS control entity may have a priori knowledge that additional media capabilities shall be added to a SDP negotiation. Therefore, the SDP Offer which arrives at UE2 includes the media capabilities of both UE1 and the resource functions.

This latter approach entails that the resource function shall pre-allocate resources for both endpoints during the session establishment, regardless they are eventually used or not. More importantly, it speeds up the session establishment process since only one unique SDP Offer-Answer between SMRF and UE2 is required. Therefore, only the proactive approach will be considered in this paper.

Fig. 3 illustrates the main steps in the proposed proactive session establishment procedure. In the proposed solution, the SMRF is able to include new media characteristics at two levels: additional media codecs and additional media security mechanisms that are supported by the MRF and the SecRF respectively. It is assumed that the SMRF is configured to detect if additional media characteristics shall be added to a SIP dialog, but without a priori knowledge of the specific media formats shared between UE1 and UE2. These assumptions are considered as a standard configuration where a call manager applies this process to dialogs between different administrative domains, but without knowing the specific media codecs and media security mechanisms methods used in each domain. In the proposed context, the SMRF is required to gather additional media codecs and media security capabilities that are supported by the MRF (represented by "C2, …") and the SecRF (represented by "K2, …") respectively. Therefore, the new SDP Offer which is sent to UE2 includes extra media options for it to choose from.

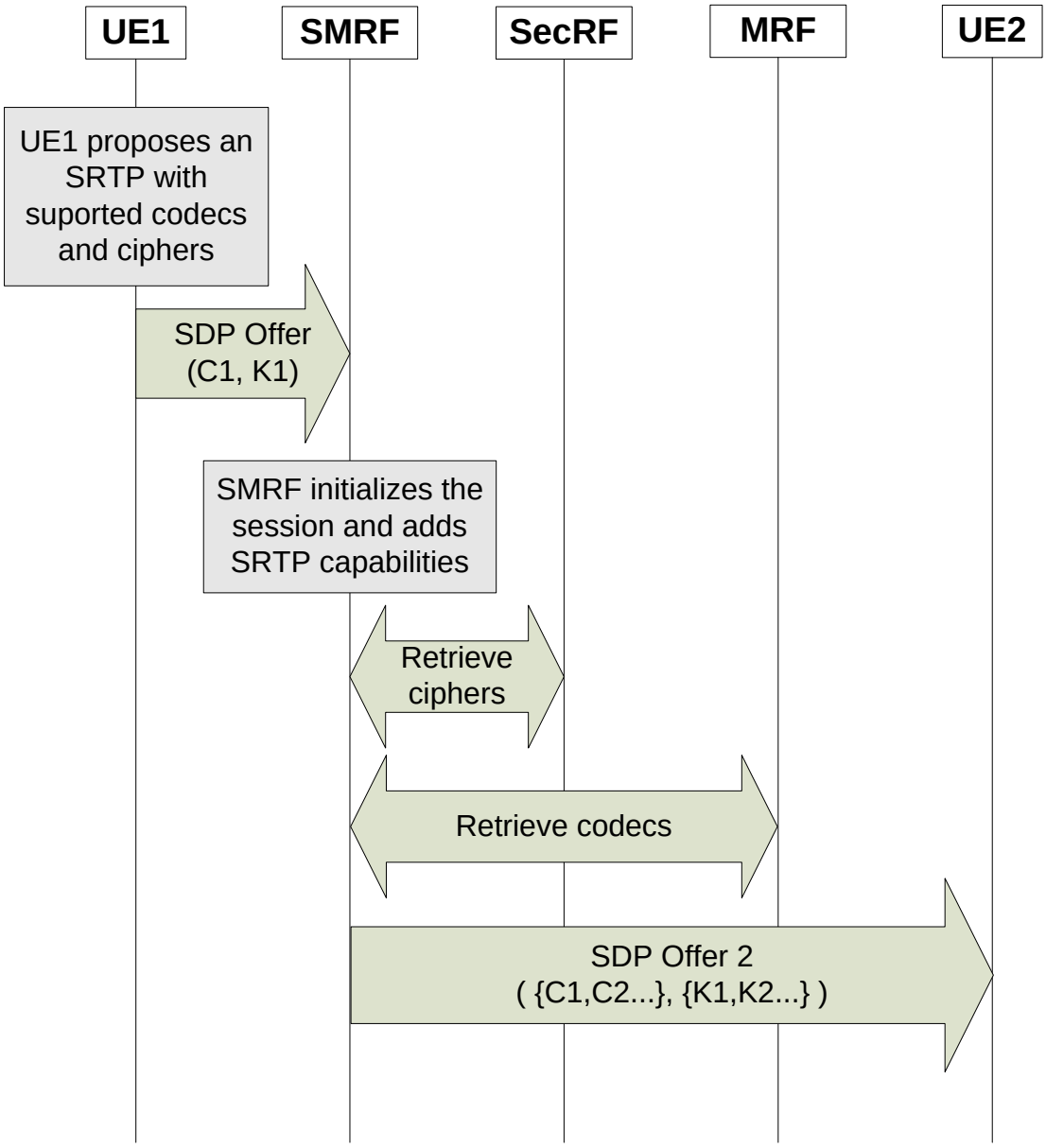

Fig. 3 Session initialization by SMRF

2.2 Session setup process: agreeing media capabilities

Once the SDP Offer is received by UE2, it shall choose a unique set of media characteristics for the session. UE2 may select any combination of codec and ciphering mechanism from those offered by UE1 and the resource functions. Depending upon the received SDP Answer from UE2, the SMRF will perform accordingly in the following situations:

- Case 1 - UE2 supports C1 and K1 offered by UE1 (Fig. 4). In this case, the resource functions are not eventually needed and the SRTP communication is established directly between UE1 and UE2.
- Case 2 - UE2 only supports C1 from UE1 and K2 from SecRF (Fig. 5). In this case, the SecRF is instructed by the SMRF to provide ciphering support and operates as a media-plane endpoint for each actual IMS user.
- Case 3 - UE2 only supports C2 from MRF and K2 from SecRF (Fig. 6). In addition to the ciphering process at the SecRF, the SMRF configures the transcoding functions at the MRF. As a result, the SecRF acts as a media-plane endpoint for both IMS users and the MRF.
- Case 4 - UE2 only supports C2 from MRF and K1 from UE1 (Fig. 7). The MRF is required for the transcoding purpose in the media plane. Also, the SecRF has to be included as well in order to obtain the plain-text media for the MRF despite both endpoints utilize the same media ciphering mechanism. From a media plane perspective, the map of connections between nodes is the same than in the previous situation.

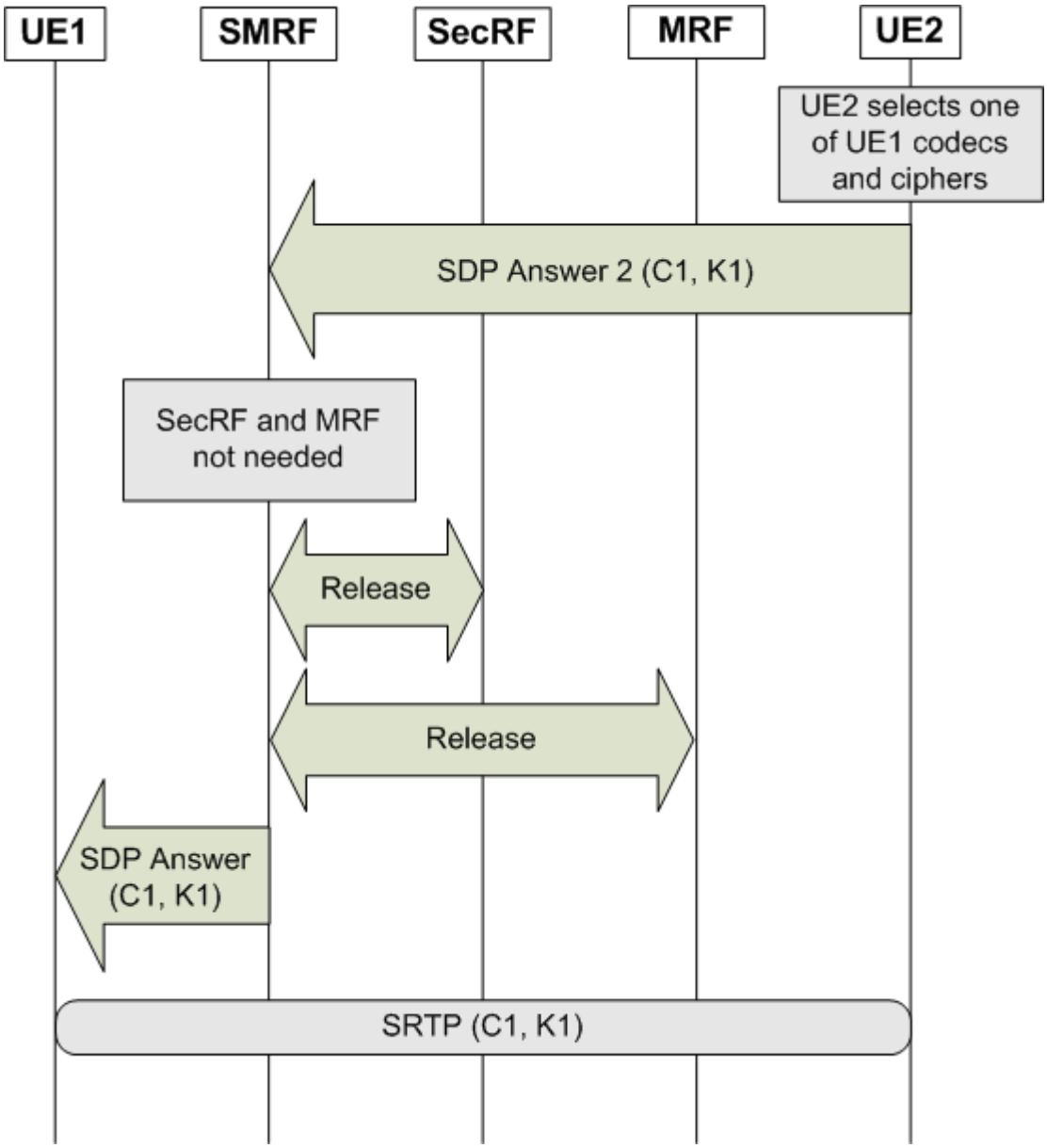

Fig. 4 Session establishment: direct mode

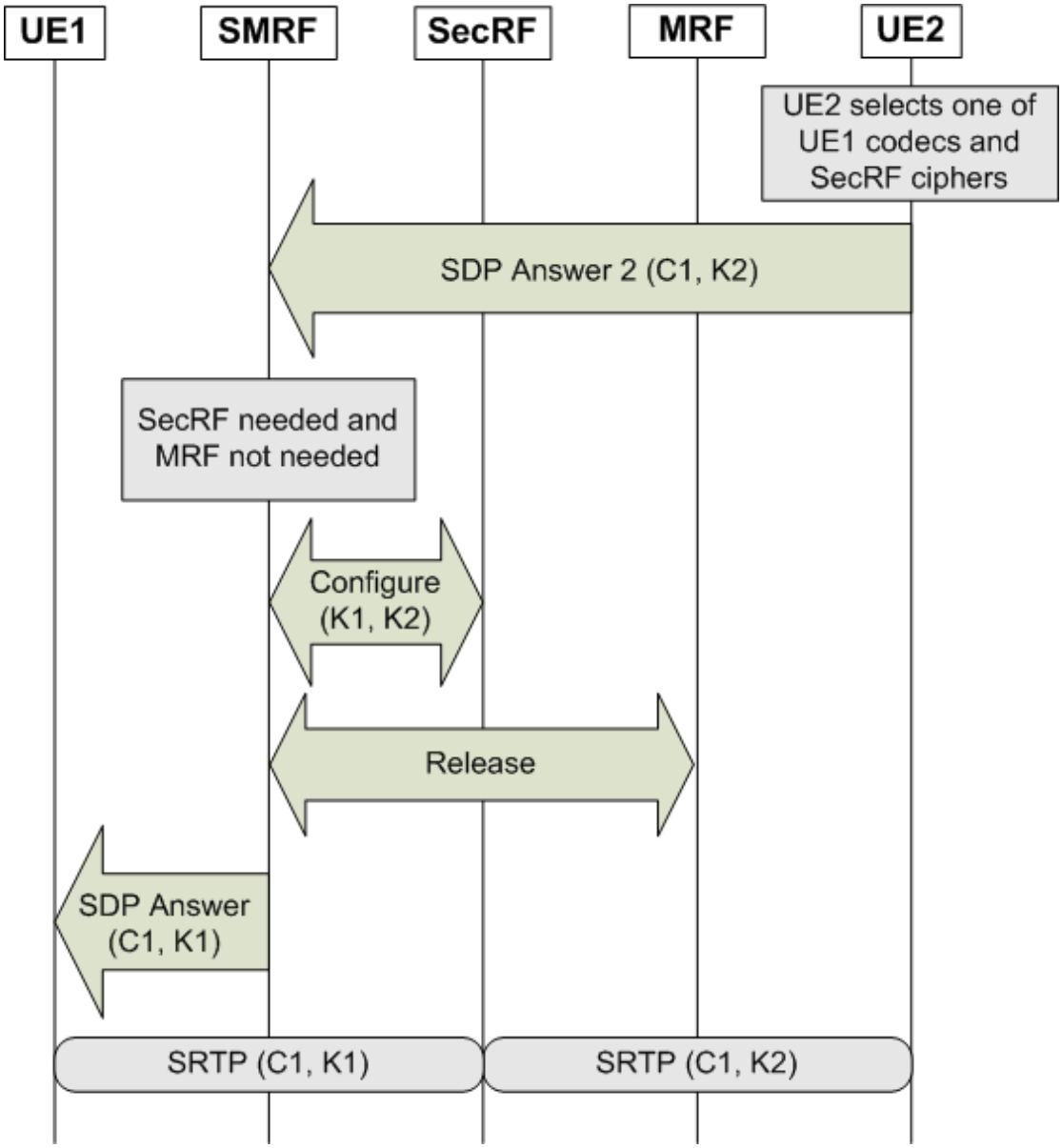

Fig. 5 Session establishment: incompatible media ciphering

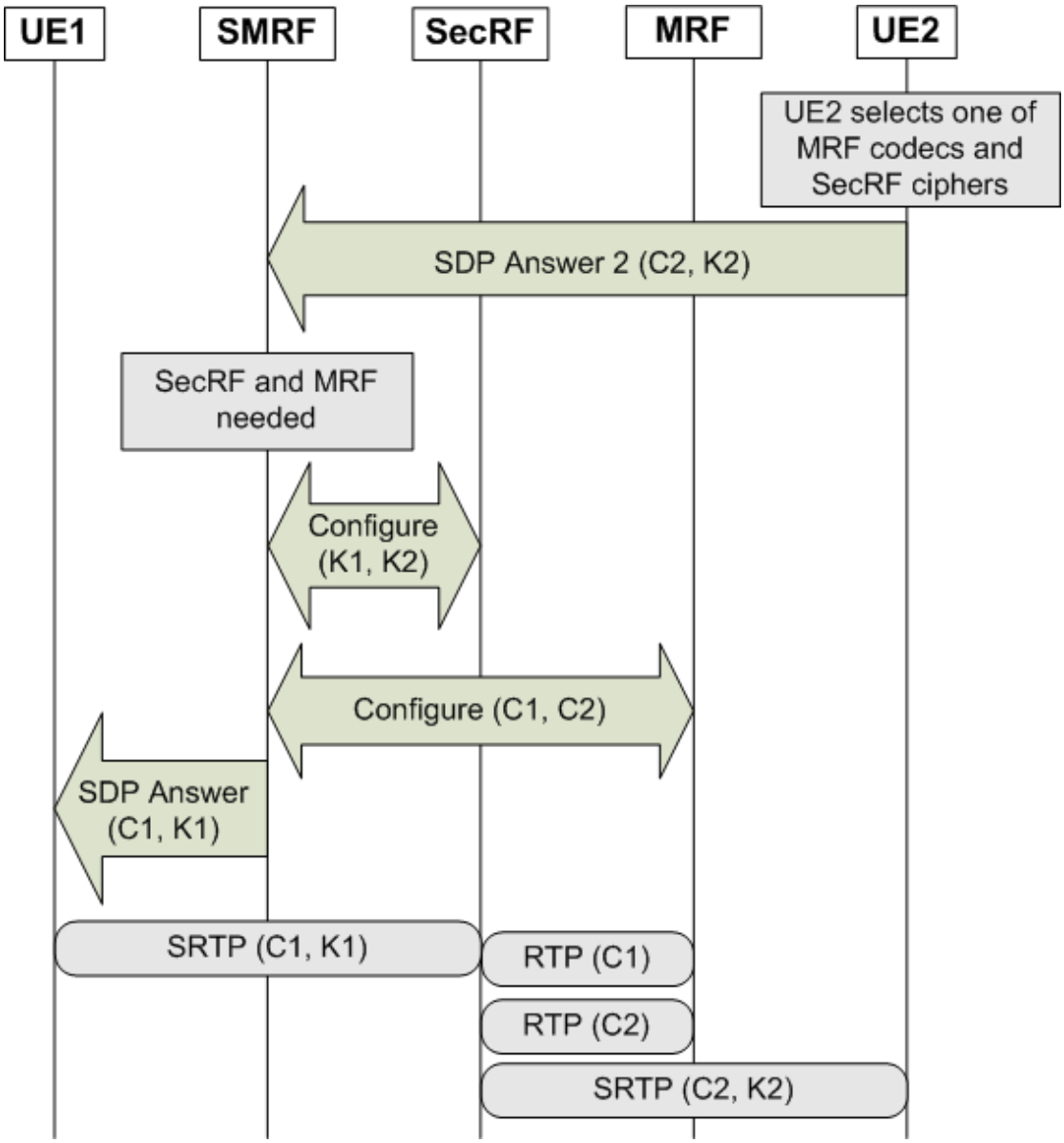

Fig. 6 Session establishment: incompatible media ciphering and codec

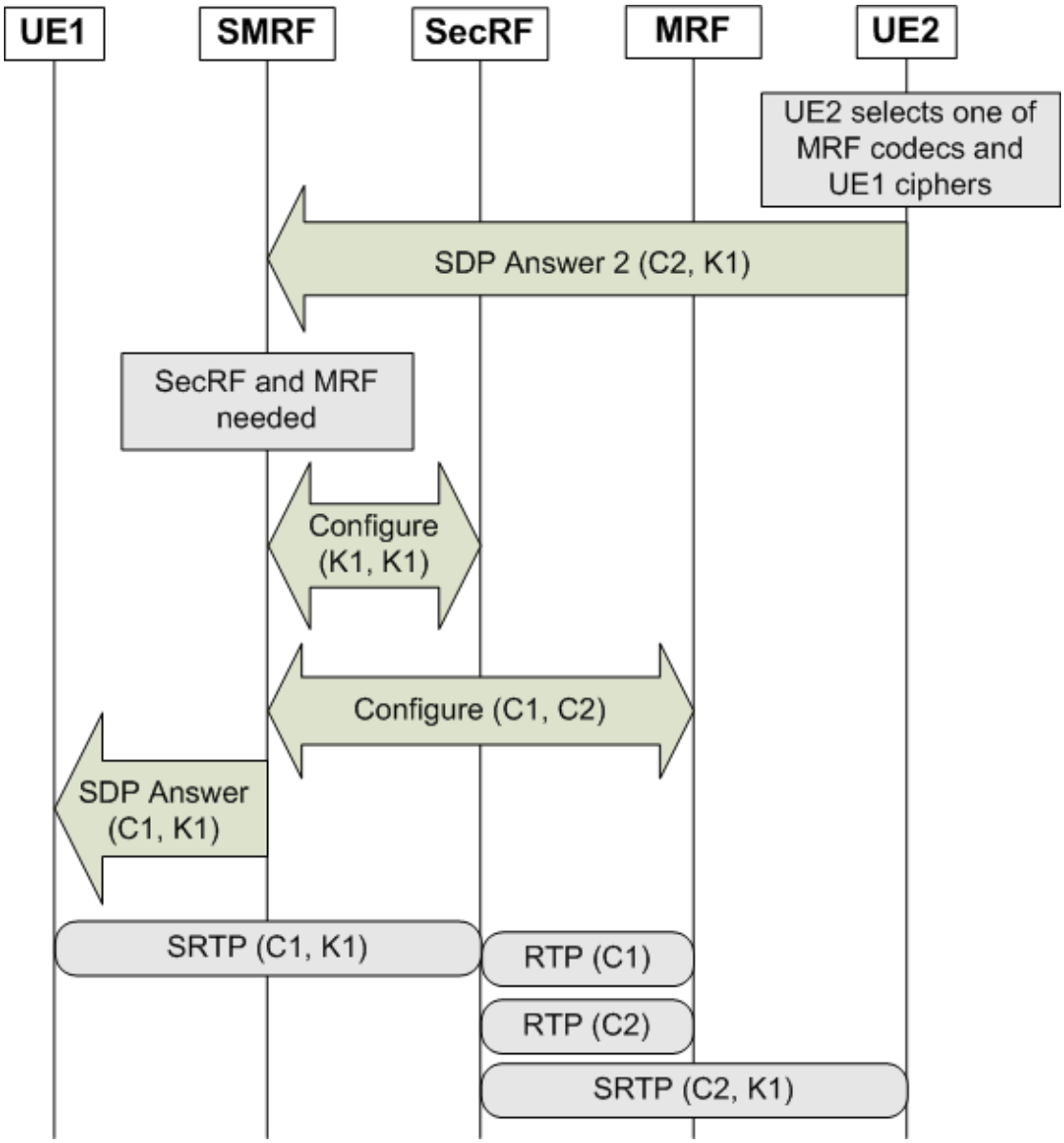

Fig. 7 Session establishment: incompatible media codec

The final configuration of the media plane is seamless for the IMS endpoints. UE2 and UE1 receive the media configuration in the SDP Offer and Answer respectively. Each media line in the SDP message includes the media characteristics and the IP address and ports of the other party, regardless of whether it is the actual counterpart endpoint or an operator-managed node. Therefore, the inclusion of trusted intermediate nodes in the media path is transparent for end users.

The previous cases illustrate the situation where the SMRF is used to reassure the media-plane compatibility between different heterogeneous endpoints. Depending of the media-level incompatibility, the SMRF AS will force the inclusion of the SecRF and/or the MRF in the media path.

Additionally, the proposed system can be configured to always force the use of the media-plane elements regardless of the compatibility of the endpoints. This operating mode is useful for enabling lawful interception / recording of the communication. The system configuration of this scenario is illustrated in Fig. 8.

- Case 5 - UE2 supports C1 and K1 offered by UE1 but legal interception is enabled. As can be observed, the SMRF AS needs to configure the SecRF and the MRF to be inserted in the media plane even when UE2 supports C1 and K1 offered by UE1. In this way, the SecRF will be implemented with the same crypto suites for the two endpoints and the MRF will be configured in a pass-through mode from the endpoints' perspective.

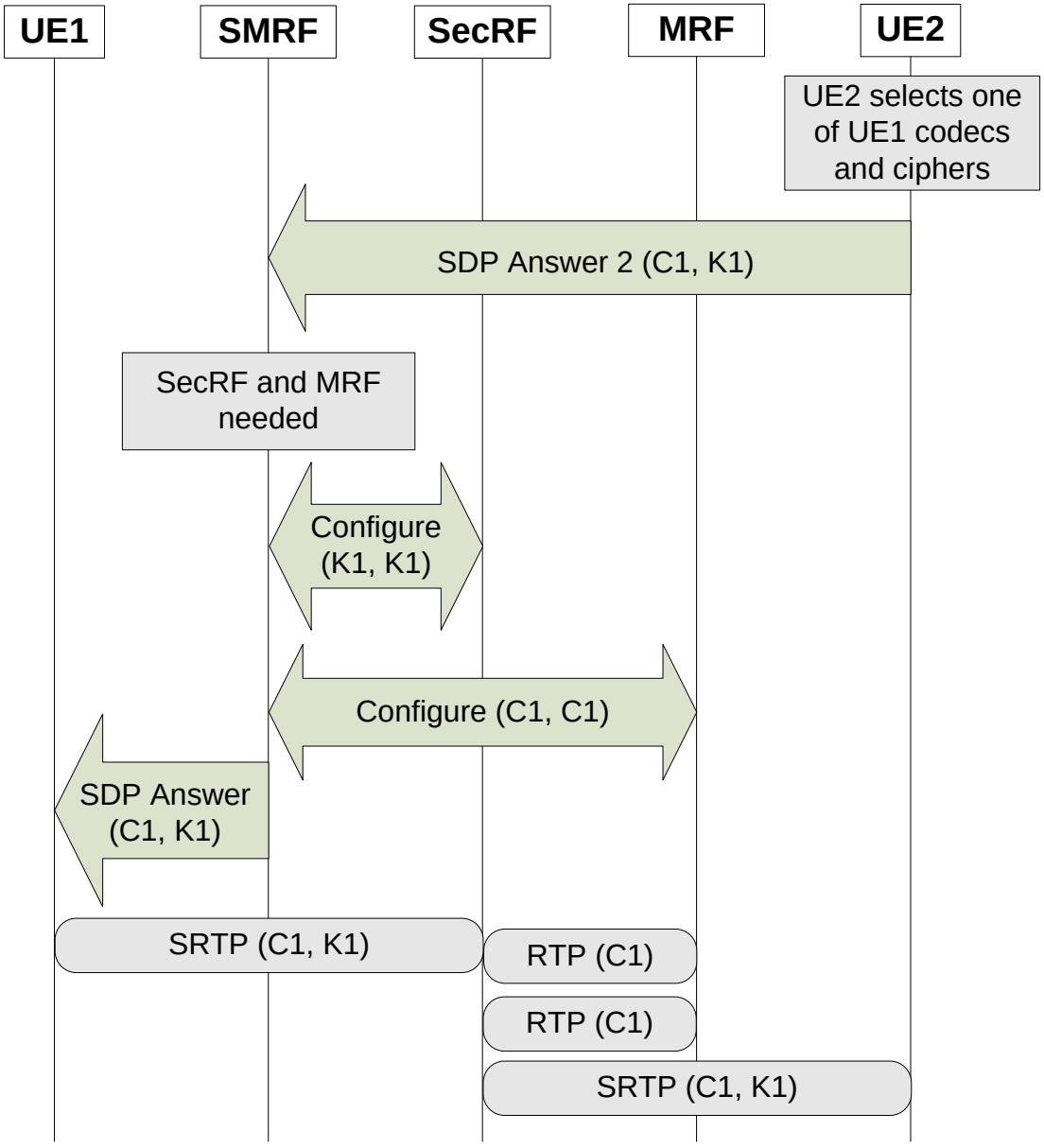

Fig. 8 Session establishment: compatible media ciphering and codec with legal interception enabled

3 Security Resource Function

The SecRF is responsible for providing media security related functions when ciphering assistance is required. The SecRF is further divided into a Security Resource Function Processor and a Security Resource Function Controller, both of them will be described thoroughly in the following sections.

3.1 Security Resource Function Processor

SecRFP is a media plane node that transparently provides ciphering support (i.e. decrypt and encrypt SRTP streams) for incompatible endpoints, allowing them to establish the communication at the media level but without compromising the security. The SecRFP is designed to work in different modes to cope with the different cases as described in Section 2.2:

- Cross-ciphering operating mode: endpoints employ different security mechanisms regardless their codec compatibility (cases 2 and 3). In this mode, the SecRF will be able to decipher the media from UE1 and cipher it again in a suitable format for UE2.
- Mono-ciphering operating mode: endpoints utilize the same security mechanisms but the MRF is needed for transcoding or recording (cases 4 and 5). In this mode, the SecRF will be required for extracting the plain text media from one endpoint, interfacing with the MRF for obtaining a new media configuration, and ciphering it again for the other endpoint with the same cryptographic suite.

In order to provide various ciphering supports, the SecRFP should be equipped with a wide range of crypto suites and key exchange solutions that are utilized by the SRTP as described in the following subsections.

3.1.1 Crypto suites of SecRFP

A crypto suite is a combination of encryption and message authentication code (MAC) algorithms that provide confidentiality, integrity and authentication for data. The default encryption method for SRTP is the Advanced Encryption Standard (AES), which can operate in two modes: Segmented Integer Counter Mode (AES_CM) and f8-mode [11]. Meanwhile, the default message authentication and integrity method for the SRTP is HMAC-SHA1 [11]. By utilizing the combination of encryption methods, message authentication and integrity solutions, in addition to various key lengths, a number

of crypto suites can be obtained (as illustrated in Table 1) [8, 25]; all of which shall be supported by the SecRFP. Furthermore, it is envisaged that the SecRFP should also provide support for future releases of crypto suites for the SRTP, enabling future compatibility and longevity of the system.

Table 1 Crypto suites support at the SecRFP

Crypto suites	References
AES_CM_128_HMAC_SHA1_80	IETF RFC 4568 (July 2006) [8]
AES_CM_128_HMAC_SHA1_32	
AES_F8_128_HMAC_SHA1_80	
AES_192_CM_HMAC_SHA1_80	IETF RFC 6188 (March 2011) [25]
AES_192_CM_HMAC_SHA1_32	
AES_256_CM_HMAC_SHA1_80	
AES_256_CM_HMAC_SHA1_32	

3.1.2 Key exchange solutions of SecRFP

A number of key exchange protocols have been proposed to manage the key exchange between endpoints to enable SRTP communication [6]. The decision as to whether the assistance of the SecRFP should be required is decided by the SMRF. Any potential key exchange protocols of the SecRFP must be indicated and initialized in the IMS signaling plane, otherwise the call which requires supported from the SecRFP cannot be established. Therefore, key management solutions that utilize the media plane for advertising their usage will not be supported by the SecRFP. Based upon these premises, several key exchange protocols with which the SecRFP shall support are illustrated in Table 2. In addition, the SecRFP should be compatible with any future key exchange solutions that also utilize the IMS signaling plane for initialization of the key management.

Table 2 Key exchange protocols support at the SecRFP

Key exchange solutions	References
SDES	IETF RFC 4568 (July 2006) [8]

MIKEY - Pre-shared key	IETF RFC 3830 (August 2004)[9], IETF RFC 6043 (March 2011) [10]
MIKEY - Public-key encryption (RSA)	IETF RFC 3830 (August 2004)[9], IETF RFC 6267 (June 2011)[26]
IMS AKA keys for media protection	3GPP TR 33.828 [6]
Otway-Rees based key management protocol	3GPP TR 33.828 [6]
ZRTP	IETF RFC 6189 (April 2011) [12]

SDP Security Descriptions for Media Streams (SDES) is a simple key management protocol that relies upon the security of the signaling plane as the key material is exchanged in the SDP negotiation process [8]. Each side of the SDP exchange includes the key by which the media sent to the other side will be protected. For this, [8] defines a new SDP "crypto" attribute that shall be understood by all the endpoints of the communication.

Multimedia Internet Keying (MIKEY) is another key management protocol defined for real-time multimedia applications [9]. The use of MIKEY in SIP signaling is defined in [10] which defines the SDP attribute "key-mgmt" with the protocol identifier "mikey". In this case, certain ciphering information is inserted in the SDP messages instead of the actual encryption key, so the user is redirected to an external system for retrieving the keying data.

MIKEY pre-shared key (MIKEY-TICKET) requires a key management server (KMS) for distributing the key material [26]. The caller requests keys and a ticket that contains a reference to the keys from the KMS and sends the ticket to the callee during the call setup phase. The callee then sends the ticket to the KMS to retrieve corresponding keys for securing the media transmission. The key transmission for MIKEY pre-shared key method is independent to the signaling plane security as the communication between individual endpoints and the KMS is protected by a pre-shared key or by a digital signature.

MIKEY-public key encryption (MIKEY-IBAKE) also requires the presence of a key management server for managing key materials [12]. Endpoints obtain their private keys from the KMS before a call setup. During the call setup process, endpoints will be informed that MIKEY-public key encryption is utilized and they will generate a security key based upon their public keys and a random number. With the purpose of a guaranteed secure delivery of private and public keys, endpoints connect the KMS via a Bootstrapping Server Function [6].

ZRTP is a media plane key management protocol utilizing a Diffie-Hellman key exchange to establish security keys for protecting media transmission [33]. Endpoints initiate the discovery phase of whether their peers also support ZRTP as soon as they obtain each other's IP address. By using basic implementations, the ZRTP cannot be utilized by the SecRFP as it does not rely upon the signaling plane for key exchange. However, [33] describes that usage of ZRTP can be advertised during a call setup phase in the signaling plane. Therefore, if this option is enabled in the signaling plane, the SecRFP should also support ZRTP.

In addition, IMS AKA keys for media protection and Otway-Rees based key management solutions also utilize signaling plane to advertise their existence [6]. As a result, the SecRFP should also support them despite they are less popular comparing with other aforementioned key exchange solutions.

By utilizing the combination of crypto suites and key management solutions, the SecRFP should provide a wide range of ciphering support for media security and/or media codec incompatible endpoints. In order to allow this to happen, the SecRFP relies upon the SecRFC to advertise its capabilities to the endpoints and also obtain media configurations of both endpoints in the signaling plane. Details of the configuration will be described in the following section.

3.2 Security Resource Function Controller

SecRFC is a signaling plane node that interprets information coming from the SMRF to control the SecRFP and also supports SIP signaling and related security aspects in order to support additional ciphering capabilities when requested. During a call setup session, the SecRFC advertises a list of ciphering capabilities of the SecRFP to the SMRF; in this way, attributes of the incoming and outgoing legs can be automatically reconfigured if the SMRF detects the need of ciphering assistance, avoiding early call termination in the signaling plane due to incompatible media security mechanisms and/or media codecs of calling parties.

Fig. 9 illustrates the SIP message flow between all the IMS entities when two UEs utilize different crypto-suites and also different key exchange solutions. For clarity purposes, the conceptual flow diagram is shown and the core IMS nodes (P/S/I-CSCF) between UEs and SMRF are not illustrated.

The SecRFC requests a set of ciphering keys and a ticket from the deployed KMS any time prior to the call setup (steps 1 and 2). During a call setup, UE1 sends the SDP Offer which contains the call session setup parameters (only security mechanism is illustrated for the demonstration purpose) towards to

UE2. The SMRF, which acts as a 3PCC, intercepts the SDP of UE1 and includes the capabilities of the SecRF (steps 4 and 5). As a result, the SDP Offer that is received by UE2 contains the capabilities of both UE1 and the SecRF.

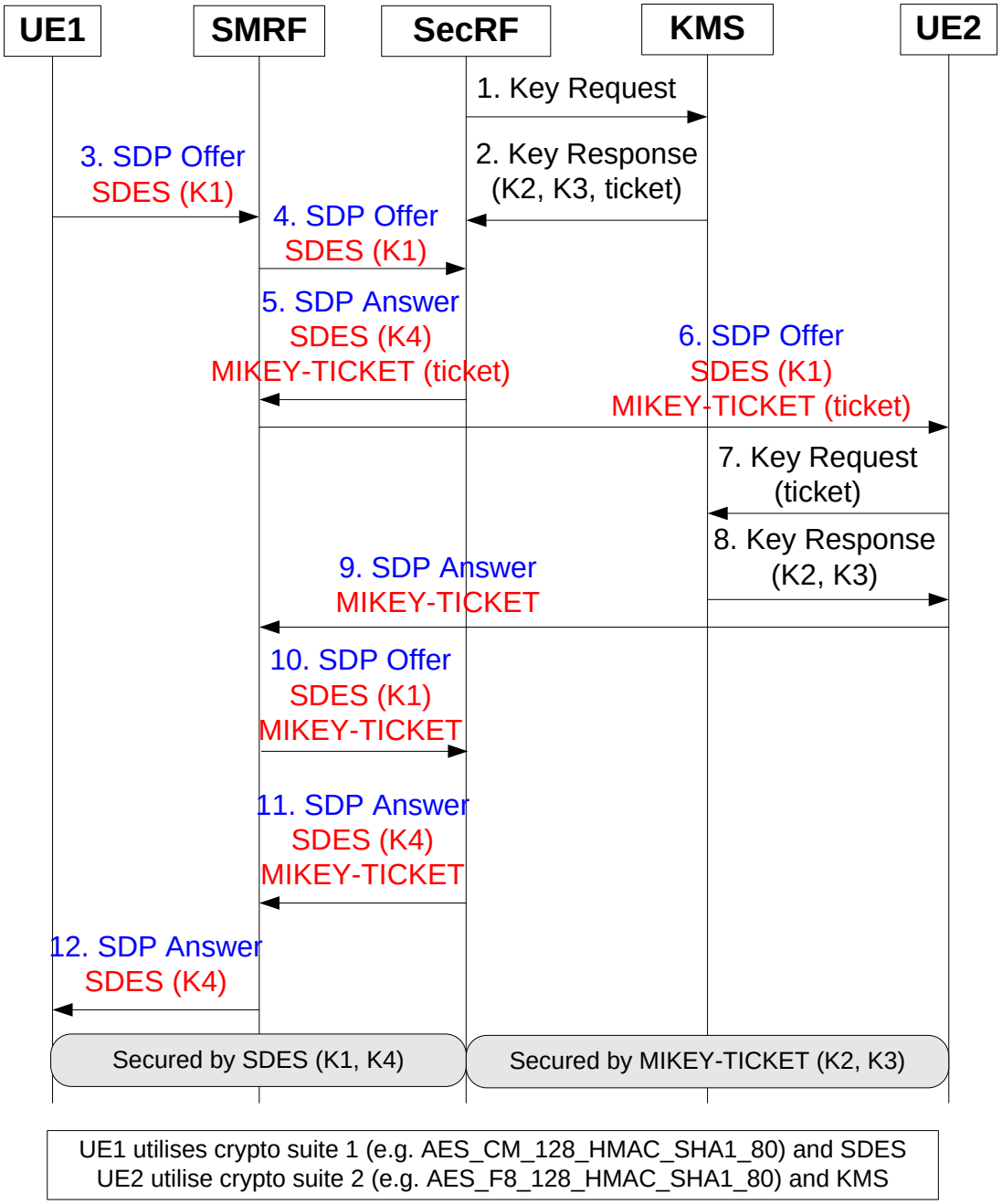

Fig. 9 Key exchange procedures and integration into the IMS signaling plane

After receiving the modified SDP Offer, UE2 selects the KMS key exchange solution and retrieves a set of keys from the KMS by presenting the received ticket (steps 7 and 8). Then, UE2 sends an SDP Answer back towards UE1. The SMRF intercepts the SDP Answer and detects if the assistance of the

SecRF is required. In this example, the ciphering support of the SecRF is essential; therefore, the SMRF sends the details of both endpoints to the SecRF and configures both legs (steps 10 and 11).

As a result, a secured communication is established between two UEs despite their security incompatibilities: the link between UE1 and the SecRF is protected by SDES and crypto suite1, while the connection between the SecRF and UE2 is secured by KMS and crypto suite2.

4 Detailed procedures for session establishment

Fig. 10 and Fig. 11 show the detailed interchange of SIP messages between all necessary IMS entities involved in the session establishment procedure with SMRF-controlled media capabilities. Particularly, Fig. 11 illustrates the high-level conceptual flow diagram of the case when both resource functions (i.e. SecRF and MRF) are required in the media path. For clarity purposes, the core IMS nodes and SIP confirmation messages such as 100 Trying or ACK are not illustrated.

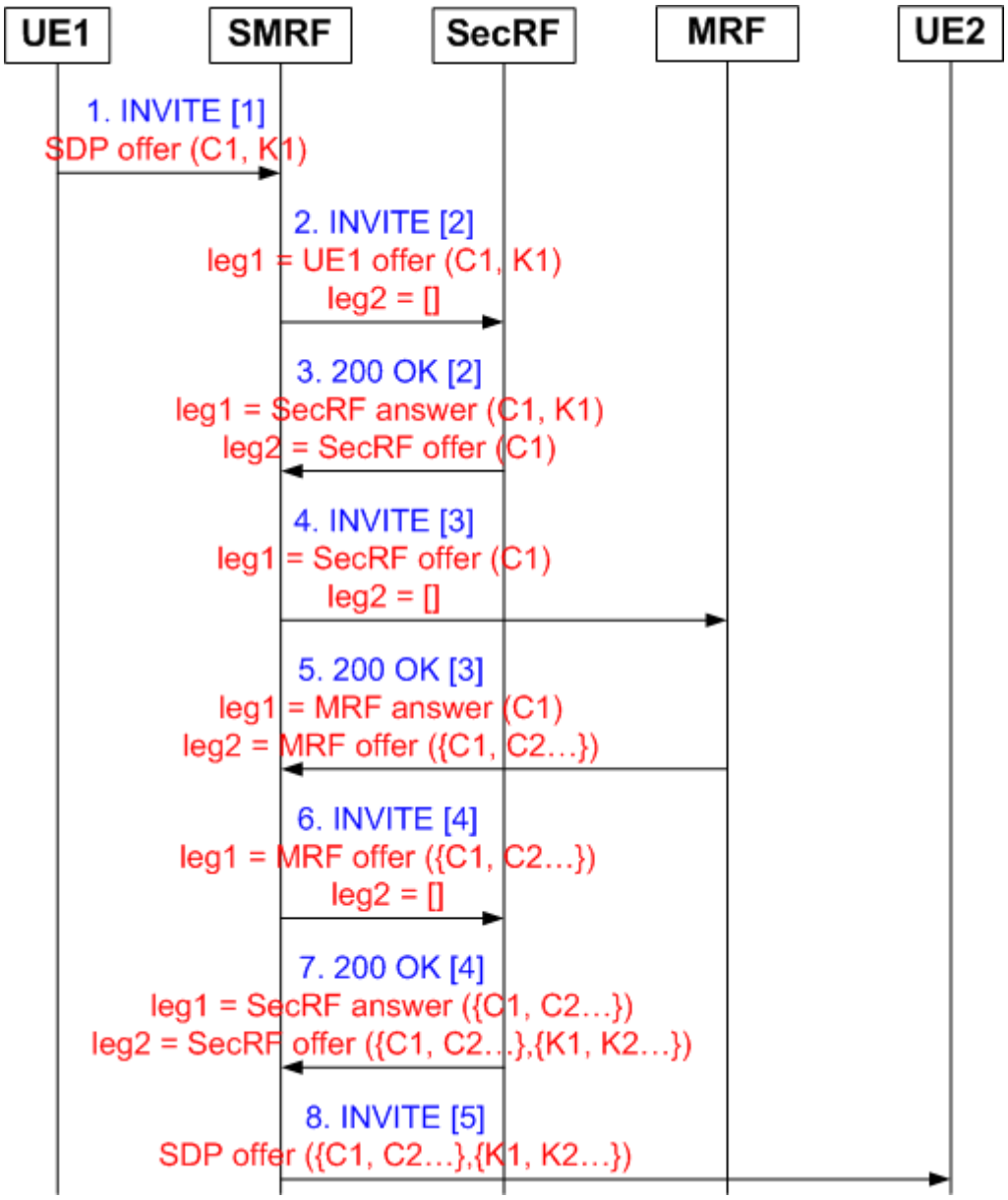

Fig. 10 SIP messages for session initialization

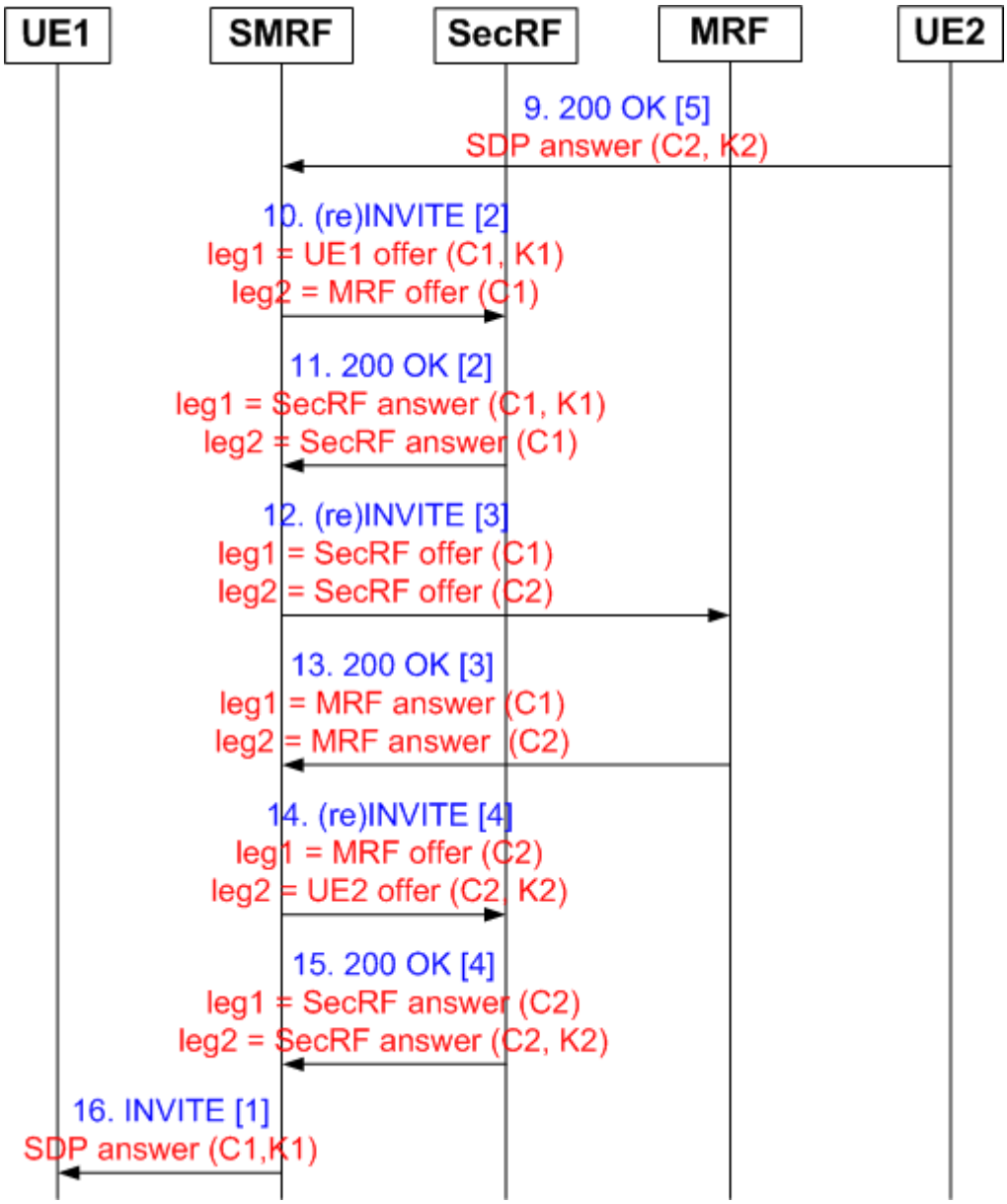

Fig. 11 SIP messages for session establishment: incompatible media ciphering and codec

Each new SIP dialog required for the whole system operation is initiated with a new SIP INVITE message. In the figures (i.e. Fig. 10 and Fig. 11), each dialog is identified with a number within square brackets after the method name. As illustrated in Fig. 10, the end-to-end SIP dialog between UE1 and UE2 is split into two dialogs by the SMRF (dialogs 1 and 5). Thus, the SMRF operates in the 3PCC mode and acts as an IMS endpoint for both UEs from the signaling standpoint. The original SDP Offer (step 1) includes a media line which defines the media type and the local port for the reception of SRTP packets, followed by the attributes describing the supported media codec (C1) and the cryptographic information (K1). The SIP interaction between the SMRF and the IMS resource functions includes two

media lines in the SDP, one for each media leg to be connected [3]. Thus, the SIP dialogs 3, 4 and 5 are used to propagate the network addresses and media characteristics for the all the pre-configured media connections. During the session initialization process the SMRF uses these dialogs to retrieve the media information from the resource functions. After the initialization process by the SMRF, the extended SDP Offer (step 8) comprises all the permutations between the supported codecs (C1, C2, …) and the supported cryptographic options (K1, K2, …) from UE1, SecRF and MRF. Upon receiving the response from UE2 (step 9), the SMRF obtains all the necessary information to configure any required media connections between UE1, SecRF, MRF and UE2 (steps 10 to 15); this is achieved by utilizing the same principle of dialogs 3, 4 and 5 to propagate the updated SDP parameters. After the configuration of the SMRF, a modified SDP answer will be sent to the UE1 to indicate the completion of the call setup process (step16); and endpoints will be able to start the communication at the media plane.

As illustrated by Fig. 10 and Fig. 11, in addition to the standard end-to-end SIP communication, a total of three new SIP dialogs are introduced and managed by the SMRF to ensure the media communication can be established between endpoints regardless their compatibilities. Fig. 12 depicts the need for these dialogs from a media plane perspective. Indeed, a number of media flows can be accurately constructed by utilizing the allocated IP addresses, network ports and media characteristics information from each involved IMS node. As illustrated by Fig. 12, each media flow is unique and essential and also they reflect the outcomes of SIP dialogs 2, 3 and 4 respectively at each resource function node.

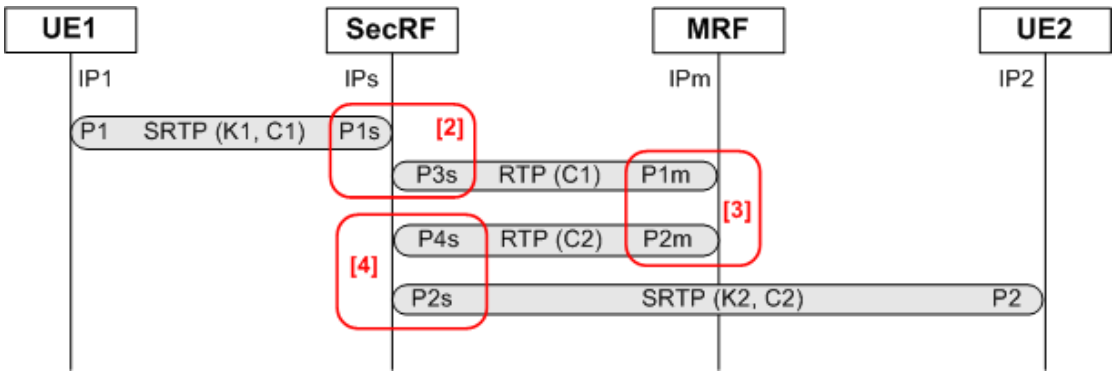

Fig. 12 Complete map of media flows and connections

In addition to the high-level SIP dialogs shown by Fig. 10 and Fig. 11, a low-level detailed SIP dialogs of how the SMRF generates the extended SDP Offer to UE2 by using the information provided by

UE1, SecRF and MRF is illustrated in Fig. 13; also, a number of codecs and cryptographic mechanisms are employed to simulate a real time SIP message exchanges scenario between the aforementioned IMS nodes. Details of these SIP dialogs are demonstrated as below:

- The SMRF receives the SDP Offer sent by UE1, which suggests that UE1 is willing to establish an SRTP voice communication with UE2 by employing a preferred set of media parameters for the codec (i.e. the Adaptive Multi-Rate (AMR)), crypto suite (i.e. AES_CM_128_HMAC_SHA1_80) and encryption key exchange method (i.e. SDES). The associated media description ID is identified as (A) in Fig. 13.
- After the interactions in dialogs 2 and 3 (not shown for clarity) the SecRF sends the SDP Answer (step 7) with the complete set of media options in the second media line (identified as (B) in Fig. 13). This media description contains all the additional codecs supported by the MRF and all the cryptographic mechanisms supported by the SecRF. In this provided example, the modified SDP Offer includes two additional Pulse Code Modulation (PCM) codecs, two extra crypto suites (i.e. AES_F8_128_HMAC_SHA1_80, AES_CM_192_HMAC_SHA1_80) and one added key exchange solutions (i.e. MIKEY-ticket) as well the media characteristics from the SDP Offer of UE1. The modified SDP offer is then sent to UE2.
- Finally, the SMRF generates the modified SDP Offer and sends it to UE2. The SDP information retrieved from UE1 (in step 1) represents the case when no resource functions are needed. From the resource functions (step 7) the SMRF can offer the situation when the two resource functions are required. Besides the SMRF generates a third option (identified as (C) in Fig. 13), which represents the case when just the security processing is necessary in the media path.

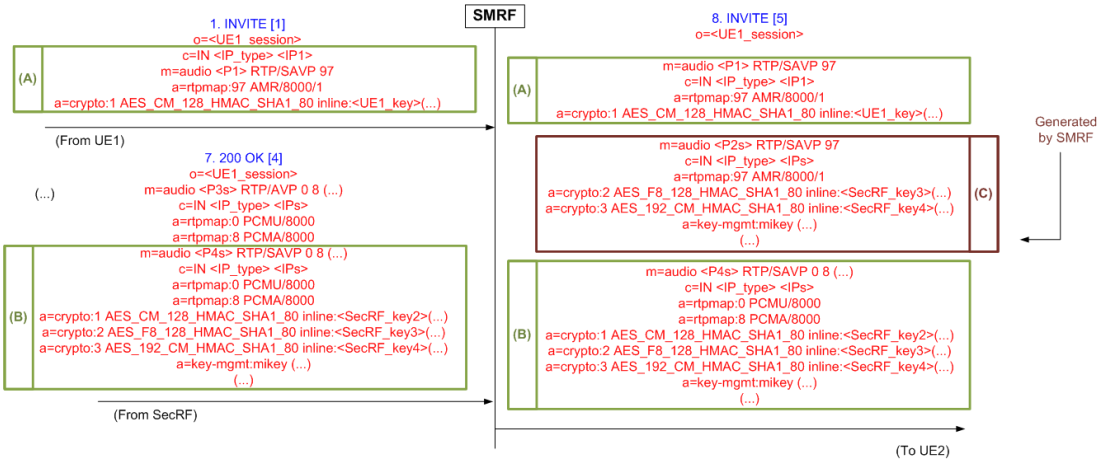

Fig. 13 Generation of extended SDP Offer by SMRF

This way, the SMRF will allocate the usage of the media resource functions based upon the response of UE2.

The previous descriptions refer to the case where the direct mode communication is enabled. If lawful interception is enabled in the system, the SMRF will always force the inclusion of the SecRF and the MRF in the media path even when no specific cross-ciphering or transcoding functions are a priori required. In that case, the first media line in Fig. 13 (identified as (A) in the figure) will not be included, and the corresponding media attributes will be also offered in the next media line (identified as (B) in the figure).

5 Performance evaluation

5.1 Analysis of the signaling overhead

In order to evaluate the impact of the proposed SMRF and SecRF upon the performance of the existing IMS signaling planes, this section discusses the number of SIP messages required by the proposed procedure in comparison to other alternatives. In total, three scenarios are designed to simulate the most extreme situations (i.e. two endpoints are fully compatible/incompatible with each other). Also both the proactive and reactive signaling approaches are considered in the case of endpoints are incompatible with each other. These three scenarios are listed as below:

1) UE1 and UE2 are compatible with each other and SMRF does not introduce additional messages in the e2e SIP signaling. This case represents the simple scenario where no additional media plane handling would be implemented.
2) UE1 and UE2 are incompatible at the media codec and ciphering mechanism, and the SMRF implements the proposed proactive scheme.
3) UE1 and UE2 are incompatible at the media codec and ciphering mechanism, and the SMRF implements a reactive scheme.

Within the scope of the proposed evaluation, the performance impact upon the existing IMS architecture is assessed by the number of additional SIP messages generated at the signaling plane. Detailed analysis of each aforementioned scenario is described as followed.

For scenario 1, upon receiving the SDP offer from UE1, the SMRF just forwards the SIP dialog towards the destination endpoint. The SDP offer/answer is made up of a set of 6 SIP methods and response codes: INVITE (SDP) – Ringing – PRACK - 200 OK (PRACK) – 200 OK (SDP) - ACK messages. According to Fig. 2, this set of messages traverses the following nodes: UE1 – P-CSCF – S-CSCF- SMRF – S-CSCF – P-CSCF –UE2, and thus 6 SIP messages are required for each SIP method or response message. As each INVITE message also triggers a 100 Trying message at each node, the total number of SIP messages required for this scenario is 42.

For scenario 2, the SMRF is configured to add the capabilities of the resource functions in a proactive approach, in order to provide interoperability at the IMS media plane. The dialog between UE1 and UE2 remains the same in terms of number of SIP messages. In addition, the SMRF initiates 3 new SIP dialogs with the resource functions. These dialogs are made up of the following set of methods and response messages: INVITE (SDP) –200 OK (SDP) - ACK messages. These dialogs are invoked by the SMRF twice, after the reception of the e2e INVITE (SDP) message of UE1 and 200 OK (SDP) message of UE2. Hence, a total number of 18 additional SIP messages are required for the inclusion of the resource functions, resulting on 60 SIP messages for the whole session.

Scenario 3 represents the situation where a reactive approach is implemented for solving media plane incompatibilities. In that case, upon the reception of UE1's INVITE the SMRF just forwards it to UE2. Since UE2 is not compatible with UE1, it replies with a 488 Not Acceptable message, which is followed by an ACK. Instead of forwarding that message back to UE1, the SMRF interacts with the resource functions in order to generate a new INVITE for UE2 with additional media capabilities and

the procedure follows the same principle as in the proactive case. As a result of the extra 488 Not acceptable, ACK, INVITE and 100 Trying SIP messages between SMRF and UE2, 12 additional SIP messages would be required in this scenario with a total of 72 SIP messages for the whole session.

Table 3 summarizes the number of SIP messages required for each scenario, detailing the number of interactions through the access networks and the core network. In summary, 42 SIP messages are required for a normal e2e call setup in the analyzed network scenario. With the proposed proactive approach, 18 additional SIP messages (42.86% of overhead) are required for every call setup process. All these extra messages occur between IMS core elements. For the reactive mode, a total of 72 SIP messages (71.43% of overhead) are required with extra messages both at the core and the access networks.

Table 3 Number of SIP messages required for a call setup procedure

Scenario	Access Networks	Core Network	Total
1. Direct mode with compatible endpoints.	14 SIP messages	28 SIP messages	42 SIP messages
2. Proactive mode.	14 SIP messages	46 SIP messages	60 SIP messages
3. Reactive mode.	18 SIP messages	54 SIP messages	72 SIP messages

In order to analyze the real impact of the signaling overhead in an IMS system, it must be noted that there are two alternative operating modes for the SMRF. On one hand, the SMRF could implement the proactive approach for every call setup regardless the compatibility of the endpoints. In this case, the number of required signaling messages is always the same for each call setup procedure. On the other hand, the SMRF could progress the initial SIP INVITE and implement the reactive approach just when required by the called endpoint. Consequently, the average number of signaling messages per call setup will depend on the ratio of sessions with compatible and incompatible endpoints. As a result, the optimal configuration of the system would depend on the specific use case scenario and specifically on the ratio of communications that eventually need the assistance of the resource functions.

In addition to the raw average number of messages per call setup, the average call setup times may also be of interest. In this sense, it must be noted that SIP messages within the core network usually exhibit better performance values in terms of message transmission speed, especially when endpoints are

connected through wireless Internet accesses. Therefore, considering the number of extra signaling messages both at the access and core segments, it is expected that the proposed proactive-based system always minimizes the maximum call setup delays for mobile endpoints with incompatible media plane characteristics.

5.2 Experimental results on the signaling plane

A prototype implementation of the SMRF element has been developed to evaluate the proposals presented in this paper. The SMRF was implemented based on the SIP Express Media Server (SEMS) project; also, modifications were carried out to extend B2BUA capabilities of the SEMS to incorporate the handling of the different resource functions. This implementation enables the evaluation of the impact by the proposed proactive approach for media plane compatibility reassurance, and specifically to analyze the latency due to the specific SMRF operations.

For the testbed scenario, the SMRF is deployed as an AS in an IMS infrastructure based on the FOKUS Open Source IMS Core project, where all the core IMS nodes are deployed in individual hardware machines. During a first set of tests, dummy endpoints and resource functions have been developed with the Open Source SIPp test tool. Thus, the roles of UE1, UE2, SecRF and MRF are emulated in the IMS infrastructure. Fig. 14 shows the main steps of the whole call setup process and the delays measured for each step.

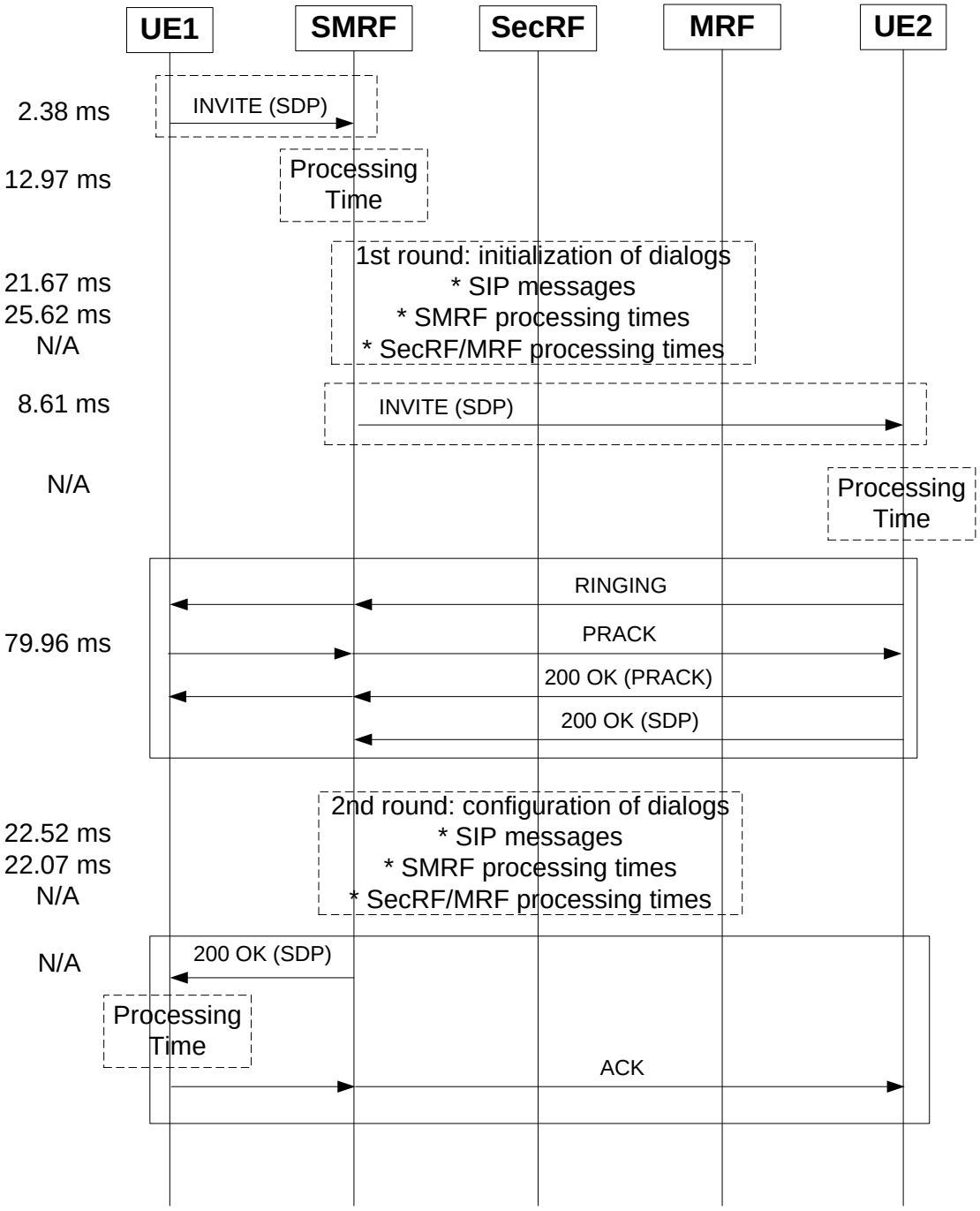

Fig. 14 Experimental latency of different call setup steps

As can be observed, the total time elapsed due to SMRF processing and to additional messages between SMRF and the resource functions is below 100 ms. The final impact of this elapsed time on the experienced call setup performance would depend on the context of use and on the total setup times due to other transmission/processing delay contributions. The processing times related to the endpoints, SecRF and MRF SIP engines are not considered in this initial experimental study. Yet, it shall be

expected that their processing times are lower than the SMRF latencies since their processing logic is less complex than their counterpart of the SMRF.

Also, a set of tests have been performed with actual endpoint devices to include the effect of the UE's processing times. Specifically, two Boghe IMS clients have been configured in the IMS infrastructure. In a first test call, the two IMS clients are configured to support the same codecs and SRTP options, while the SMRF is configured to disable the invocation of the resource functions. The measured call setup time in this direct call setup is around 450 ms. Next, one of the clients is configured with different media plane options and the SMRF is configured to enable the use of resource functions. In this case, the total call setup time measured is in the range of 530 ms. Thus, it can be inferred that the overhead of the proposed SMRF operations is in the range of 80 ms, which in this case represents the 17% of time overhead. Once again, the total call setup times and the ratio of overhead introduced by the proposed operating mode depend on the context of use, such as the type of access network used by the endpoints.

6 Conclusions

The protection of the media flows is critical for every IMS-based services such as personal communications, professional and emergency communications, content distribution on mobile e-commerce, etc. This paper proposes a complete solution that copes with the functional requirements for including a trusted network-operated resource function in a secured media path. As possible future media protection research areas, advanced digital rights management techniques shall be considered to protect unauthorized media distribution even from those users allowed to access the media flows [14]. As well, advanced key agreement mechanisms for multiparty communications shall be taken into account [30].

For media recording purposes, such as lawful interception, the media packets can be just captured, decrypted and derived to a network function. If the system is aimed at providing the standardized media transcoding functions, the clear-text media shall be processed and then once again encrypted and sent to the destination endpoint. This situation is supported by the e2m2e solution proposed in this paper, identified as mono-ciphering operating mode. As a step beyond state-of-the art solutions, the proposed solution also allows the system to implement cross-ciphering operations in the IMS resource function. This way, the IMS architecture is endowed with a functional entity that is able to reassure

secured communications even if the endpoints do not share common security mechanisms. This feature is traditionally considered of utmost importance in network infrastructures devoted to critical communications, in order to support emergency operations in multi-organization cooperative environments.

The overall architecture is designed as an adaptable and extensible system, which allows seamless integration into standardized IMS infrastructures. The proposed SMRF entity is introduced into the IMS signaling plane as an Application Server, and interfaces with the core S-CSCF through the standard ISC reference point. This way, those functionalities have been extracted in this proposal to an external control node in order not to require mandatory modifications in the IMS standards. However, from a general perspective these functionalities could be directly included at the IMS control elements such as the S-CSCF without affecting their normal operation.

Additionally, the SMRF is designed to manage the operation of the different media-plane resource functions independently. As can be observed, the specialized entities for processing the media content and the media encryption are kept separated. This way, the SMRF is able to include them both in the path individually or in a cooperative manner, depending on the necessary functionalities.

From the perspective of the system performance, the selected proactive approach reduces the latency in the session establishment compared to the alternative reactive approach. Furthermore, the proactive addition of capabilities in the SDP Offer reassures the establishment of the communication between a priori incompatible devices.

In future, prototypes of fully functional SMRF and SecRF will be developed and their impacts upon the IMS signaling and media planes will be thoroughly analyzed.

Acknowledgments

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement 284863 (FP7 SEC GERYON).

References

1. 3rd Generation Partnership Project (2000-). IP Multimedia Subsystem (IMS); Stage 2. Technical Specification 23.228. 3GPP. http://www.3gpp.org/ftp/Specs/html-info/23228.htm. Accessed 28 September 2010.

2. 3rd Generation Partnership Project (2001-). 3G security; Access security for IP-based services. Technical Specification 33.203. 3GPP. http://www.3gpp.org/ftp/Specs/html-info/33203.htm. Accessed 20 December 2010.

3. 3rd Generation Partnership Project (2001-). IP Multimedia (IM) session handling; IM call model; Stage 2. Technical Specification 23.218. 3GPP. http://www.3gpp.org/ftp/Specs/html-info/23218.htm. Accessed 10 July2010.

4. 3rd Generation Partnership Project (2002-). 3G security; Network Domain Security (NDS); IP network layer security. Technical Specification 33.210. 3GPP. http://www.3gpp.org/ftp/Specs/html-info/33210.htm. Accessed 16 June 2010.

5. 3rd Generation Partnership Project (2009-). IP Multimedia Subsystem (IMS) media plane security. Technical Specification 33.328. 3GPP. http://www.3gpp.org/ftp/Specs/html-info/33328.htm. Accessed 20 December 2010.

6. 3rd Generation Partnership Project (2009-2012). IP Multimedia Subsystem (IMS) media plane security. Technical Report 33.828. 3GPP. http://www.3gpp.org/ftp/Specs/html-info/33828.htm. Accessed 20 December 2010.

7. Aloudat, A., & Michael, K. (2011). Toward the regulation of ubiquitous mobile government: a case study on location-based emergency services in Australia. Electronic Commerce Research, 11(1), 31–74.

8. Andreasen, F., Baugher, M., & Wing, D. (2006). Session Description Protocol (SDP) Security Descriptions for Media Streams. RFC 4568. IETF. http://www.ietf.org/rfc/rfc4568.txt. Accessed 8 June 2012.

9. Arkko, J., Carrara, E., Lindholm, F., Naslund, M., & Norrman, K. (2004). MIKEY: Multimedia Internet KEYing. RFC 3830. IETF. http://www.ietf.org/rfc/rfc3830.txt. Accessed 8 October 2012.

10. Arkko, J., Naslund, M., Norrman, K., & Carrara, E. (2006) Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP). RFC 4567. IETF. http://www.ietf.org/rfc/rfc4567.txt. Accessed 8 June 2012.

11. Baugher, M., McGrew, D., Naslund, M., Carrara, E., & Norrman, K. (2004). The Secure Real-time Transport Protocol (SRTP). RFC 3711. IETF. http://www.ietf.org/rfc/rfc3711.txt. Accessed 15 March 2010.

12. Cakulev, V., & Sundaram,G. (2011). MIKEY-IBAKE: Identity-Based Authenticated Key Exchange (IBAKE) Mode of Key Distribution in Multimedia Internet KEYing (MIKEY). RFC 6267. IETF. http://www.ietf.org/rfc/rfc6267.txt. Accessed 8 October 2012.

13. Chang, K.-D., Chen, C.-Y., Chen, J.-L., & Chao, H.-C. (2010) Challenges to Next Generation Services in IP Multimedia Subsystem. *Journal of Information Processing Systems*, 6(2), 129-146.

14. Chen, X., & Lian, S. (2011). Service and P2P based secure media sharing in mobile commerce environments. Electronic Commerce Research, 11(1), 91–101.

15. Dolan, M.F., Tatesh, S., Casati, A., Tsirtsis, G., Anchan, K., & Flore, D. (2012) LTE for public safety networks. *IEEE Communications Magazine*, 51(2), 106-112.

16. Forsberg, D., Horn, G., Moeller, W.-D. & Niemi, V. (2010) Security for Voice over LTE. In *LTE Security* (pp. 201-214). Chichester, UK: John Wiley & Sons.

17. Floroiu, J., & Sisalem, D., (2009). A comparative analysis of the security aspects of the multimedia key exchange protocols. Proceedings of the 3rd International Conference on Principles, Systems and Applications of IP Telecommunications. doi:10.1145/1595637.1595640.

18. Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., Gritzalis, S., Ehlert, S., & Sisalem, D. (2006) Survey of security vulnerabilities in session initiation protocol. *IEEE Communications Surveys & Tutorials*, 8(1), 68-81.

19. Gurbani, V. K., & Kolesnikov, V., (2011) A Survey and Analysis of Media Keying Techniques in the Session Initiation Protocol (SIP). *IEEE Communications Surveys & Tutorials*, 13(2), 183-198.

20. Hunter, M. T., Clark, R. J., & Park, F. S. (2007) Security issues with the IP multimedia subsystem (IMS). Proceedings of the 2007 Workshop on Middleware for next-generation converged networks and applications. doi: 10.1145/1376878.1376887.

21. Kambourakis, G., Kolias, C., Gritzalis, S., & Park, J.-H. (2011). DoS attacks exploiting signaling in UMTS and IMS. *Computer Communications*, 34(2011), 226–235.

22. Keromytis, A.D., (2012) A Comprehensive Survey of Voice over IP Security Research. *IEEE Communications Surveys & Tutorials*, 14(2), 514-537.

23. Manzer, E. (2012). Evolution and deployment of VoLTE (Voice-over-Long-Term-Evolution). *e & i Elektrotechnik und Informationstechnik*. doi: 10.1007/s00502-012-0049-5.

24. Mascha, M. F., Miller, C. L., & Janvrin, D. J. (2011). The effect of encryption on Internet purchase intent in multiple vendor and product risk settings. Electronic Commerce Research, 11(4), 401–419.

25. McGrew, D. (2011). The Use of AES-192 and AES-256 in Secure RTP. RFC 6188. IETF. http://www.ietf.org/rfc/rfc6188.txt. Accessed 8 June 2012.

26. Mattsson, J., & Tian, T. (2011). MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY). RFC 6043. IETF. http://www.ietf.org/rfc/rfc6043.txt. Accessed 8 October 2012.

27. Onofrei, A. A., Rebahi, Y., & Magedanz, T. (2010) Preventing Distributed Denial-of-Service Attacks on the IMS Emergency Services Support through Adaptive Firewall Pinholing. *International Journal of Next-Generation Networks*. 2(1), 1-17.

28. Petrova, K., & Wang, B. (2011). Location-based services deployment and demand: a roadmap model. Electronic Commerce Research, 11(1), 5–29.

29. Rosenberg, J., & Schulzrinne, H. (2002). An Offer/Answer Model with the Session Description Protocol (SDP). RFC 3264. IETF. http://www.ietf.org/rfc/rfc3264.txt. Accessed 15 March 2010.

30. Tan, Z. (2012). An efficient identity-based tripartite authenticated key agreement protocol. Electronic Commerce Research, 12(4), 505–518.

31. The Global mobile Suppliers Association (2010). Evolution to LTE. Report. GSA. http://www.gsacom.com/downloads/pdf/GSA_Evolution_to_LTE_report_011112.php4. Accessed 10 November 2012.

32. Vrakas, N., Geneiatakis, D., Lambrinoudakis, C. (2013). Evaluating the Security and Privacy Protection Level of IP Multimedia Subsystem Environments. *IEEE Communications Surveys & Tutorials*. doi: 10.1109/SURV.2012.072412.00169.

33. Zimmermann, P., Johnston, A. (Ed.), & Callas, J. (2011). ZRTP: Media Path Key Agreement for Unicast Secure RTP. RFC 6189. IETF. http://www.ietf.org/rfc/rfc6189.txt. Accessed 11 November 2012.

Jose Oscar Fajardo works as research fellow in the Department of Communications Engineering of the University of the Basque Country (UPV/EHU), at the Faculty of Engineering in Bilbao. He received his M.Sc degree in 2003 and he is now Ph.D. candidate. He has lately worked in the FP7 ICT ADAMANTIUM (2007-2010), where he researched the adaptive management of mobile multimedia services under the framework of IMS. He has co-authored more than 25 journal and conference papers since 2005, mainly in the areas of QoS/PQoS/QoE and service performance assessment, and QoS-aware networking. His current research interest is in the use of IMS for orchestrating emergency communications over heterogeneous radio access technologies (TETRA, LTE). He is currently involved in the FP7 SEC GERYON project.

Dr. Fidel Liberal received his BS and MS in Telecommunications Engineering from the University of the Basque Country (UPV/EHU), Spain, in 2001. In 2005, he received his PhD in Telecommunications Engineering from the same university for his work in the area of holistic management of quality (both QoS and QoE) in telecommunications services. He currently works as a Lecturer and researcher in the Faculty of Engineering of Bilbao, where he currently acts as PI in the FP7 SEC GERYON project. He has co-authored more than 35 conference and journal papers.

Dr Fudong Li is a Research Fellow for GERYON project within the Centre for Security, Communications and Network Research (CSCAN) at the Plymouth University, where he previously completed a BSc(Hons.) degree in Computer System and Networks, an MRes degree on the subject of Network Systems Engineering and a PhD degree in Behaviour profiling for mobile devices. His research interests are behaviour profiling, user authentication / intrusion detection techniques for mobile devices, biometrics and network security for 3G, LTE and IMS domains.

Dr Nathan Clarke graduated with a BEng (Hons) degree in Electronic Engineering in 2001 and a PhD in 2004 from the Plymouth University. He has remained at the institution and is now an Associate Professor in Information Security and Digital Forensics within the Centre for Security, Communications and Network Research. Dr Clarke is the director of the Digital Forensics Laboratory, a specialist research facility, and heads up the regional lead for the national centre of excellence in cybercrime and forensic investigation. He is also an adjunct Associate Professor at Edith Cowan University, Western Australia. His research interests reside in the area of biometrics, forensics and intrusion detection; having published over 100 papers in international journals and conferences, books, edited books and patents. Dr Clarke is UK representative in the IFIP working groups relating to the Human Aspects of Information Security & assurance, Identity Management and Information Security Education. He has on-going collaboration in three EU FP7 projects, ECENTRE, GERYON and SPACE-DATA ROUTERS.

Dr Is-Haka Mkwawa holds a PhD in Computing from the University of Bradford. He is currently working as a research fellow within EU FP7 GERYON project at the Plymouth University. He has also been working in various capacities on EU FP6 and FP7 projects (e.g. ADAMANTIUM, VITAL and NoE Euro FGi) since 2002 with the Plymouth University, the University of Bradford and the University College Dublin. He is the author of several refereed publications on parallel computing and communication, VoIP quality adaptations, Mobility management in mobile and wireless networks, performance analysis and evaluation of computer networks.