Master thesis

MSc Computing Science

Software Engineering & Distributed Systems

Media Security in Open IMS Core

Author: A.S. van Gelder

Supervisors: dr. F.B. Brokken, prof. dr. M. Aiello

External Supervisor: ir. F. Fransen

Date: July 2009

University of Groningen

TNO ICT

Media Security in Open IMS Core

University of Groningen
Faculty of Mathematics and Natural Sciences
Nijenborgh 9
9747 AG Groningen

TNO Information- and Communication technology
Eemsgolaan 3
P.O. Box 1416
9701 BK Groningen

Date July 2009

Author Arnaud van Gelder
Lauwersstraat 48
9725 HG Groningen
T: 06 48794370
E: arnaudvangelder@gmail.com

Student number 1338889

Supervisors Dr. F.B. (Frank) Brokken — University of Groningen
Prof. dr. M. (Marco) Aiello — University of Groningen
Ir. F. (Frank) Fransen — TNO Information- and Communication technology

Abstract

Mobile networks have evolved enormously over the last past decades and nowadays convergence with fixed networks is quite normal. However, traditional GSM networks are not suited best for the transfer of IP traffic, since technical limitations prohibit high bandwidth connections. Therefore the 3GPP developed a mobile system based on evolved GSM core networks and the radio access technologies that they support. Examples of such systems are GPRS, EDGE and UMTS. Currently they are working on the specifications of the fourth generation of mobile networks, which is based on the IP Multimedia Subsystem (IMS). IMS is an access independent framework, which is capable of delivering media services to (mobile) users. An example application is a Voice over IP connection between two connected devices, for example two smartphones. However, other media related services may be offered as well.

Since previous mobile networks had its own security mechanisms and because IMS is an evolvement of these networks, the IMS specification initially did not offer media security. Due to the growing convergence of fixed and mobile networks over the last few years the specification has already changed over time and IMS has become access network independent, which led to the term Common IMS. Because of this access network independency property, media security became a real issue, since not every access network has a security mechanism build in, e.g. cable networks. Therefore the 3GPP is looking for a solution and has already done several proposals. This thesis discusses which of the proposed solutions matches the stated 3GPP requirements best and looks how the architecture of IMS is impacted by the implementation of those solutions.

Table of Contents

1 Introduction

1.1 IP Multimedia Subsystem

The mobile and fixed networks have evolved enormously in the past few decades [1]. In the mobile world, first-generation (1G) networks were developed to transport speech and speech related data. These networks evolved into the second-generation (2G) networks, which offered some data and more sophisticated services to the end-users. Nowadays the third-generation (3G) has become the standard mobile network offering faster data rates and multimedia services.
The fixed networks have evolved from the traditional speech and connection oriented Public Switched Telephone Networks (PSTN) into an always on, high bandwidth IP based network.

Currently we are experiencing the convergence of fixed and mobile networks as the mobile market is increasing in a large extent with new devices having large amounts of memory, high colour displays, built-in cameras, wireless network connections and so on. These devices are always-on always-connected application devices and the mentioned properties make those devices suitable for high end, real-time network applications, e.g. shared browsing, shared gaming, Voice over IP.
The most important aspect of these next generation, all-IP converged networks is the ability to establish peer-to-peer connections between the new Internet Protocol (IP) enabled devices. As a consequence there must be a mechanism to reach another peer.

The IP Multimedia Subsystem (IMS) is such an architectural framework offering user endpoints (peers) the possibility to setup an IP based connection for multimedia services. In [1] IMS is defined as:
'IMS is a global, access-independent and standard-based IP connectivity and service control architecture that enables various types of multimedia services to end-users using common Internet-based protocols.'

IMS is developed by the 3rd Generation Partnership Project (3GPP) and offers an architecture enabling the convergence of data, speech and network technology over an IP based infrastructure and is designed to fill the gap between the existing telecommunications

technology and internet technology that increased bandwidth alone does not provide. Currently IMS is used next to the existing mobile networks, offering a hybrid solution, but in the Next Generation Network 4G (NGN) IMS is supposed to be the underlying technology.

IMS uses Internet Engineering Task Force (IETF) standardized protocols such as Session Initiation Protocol (SIP) to establish the connections. It is not intended to standardise applications itself, but to aid the access of multimedia and voice applications across wireless and wireline terminals.

1.2 IMS Architecture

The functionality and most global architecture of the IP Multimedia Subsystem can be represented by a figure similar to Figure 1.1. User endpoints (UE) which want to set up a media session need to contact the IMS core network using Session Initiation Protocol (SIP) messages. After negotiating media session parameters an end-to-end Real-time Transport Protocol (RTP) media session is established. A typical example of such a session is a Voice over IP session.

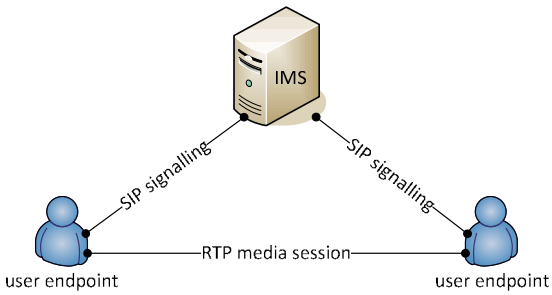

Figure 1.1 Global IMS architecture

In more detail the IMS architecture is a collection of different functions linked by standardized interfaces, which may be classified in categories and divided into the following separate layers [1]:

- the application layer
- the IMS control layer
- the transport layer

Figure 1.2 shows the design of the detailed IMS architecture. It illustrates the different IMS entities and key functions with respect to the layered design and the classification in categories and it also shows the signalling and media communication between the different

layers. Please note that connections inside a layer and between the transport layer and Application Servers are not shown.

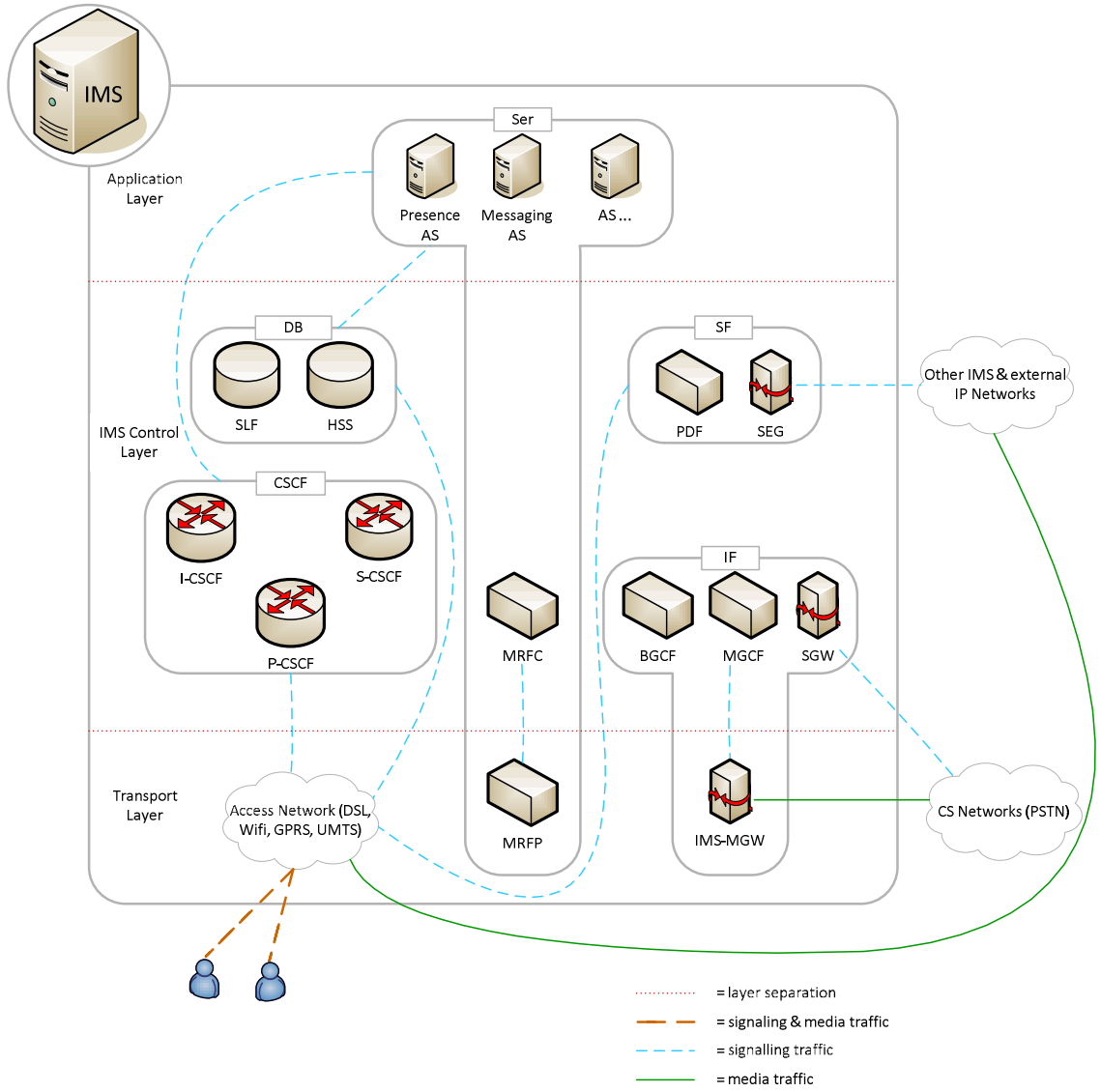

Figure 1.2 Detailed layered IMS architecture

The benefit of the layered approach is that it facilitates the addition of new access networks and application servers to the system. New access networks, like WLAN and fixed broadband have already been added to the 3GPP specifications in previous releases [1].

Figure 1.2 also illustrates the categorization of the IMS entities into five categories. The services (Ser) exist out of all IMS service-related functions, interworking functionalities (IF) categorizes the functions which handle signalling and media exchange between IMS and

Circuit Switched (CS) networks and the support functions (SF) are responsible for policy decisions and security related computation. Detailed information on these categories can be found in [1].

The Databases (DB) category exist out of the Home Subscriber Server (HSS) and the Subscription Locator Function (SLF). The HSS is the main data storage for all subscriber and service-related data of the IMS; it contains user identities (private and public), supports authentication and authorization of the users and it can provide information about the user's physical location.

The SLF is a function which maps user addresses to an HSS in the case that multiple HSS's are deployed by the network operator.

The core of the IMS architecture are the Call Session Control Functions (CSCF's). There are three different CSCF's, all having their own tasks and responsibilities, but they all participate in user registration and session establishment. Together they form the SIP routing machinery.

The Proxy Call Session Control Function (P-CSCF) is a SIP proxy that is the first contact point for users within the IMS. This means that all SIP signalling traffic from the UE will be sent to the P-CSCF and, similarly, all terminating SIP traffic from the network is sent from the P-CSCF to the UE. One of its tasks is to establish IPSec Security Associations in order to provide integrity and confidential protection for SIP signalling between UE and P-CSCF.

The Interrogating Call Session Control Function (I-CSCF) is used by the other CSCF's in order to provide the name of the next hop (either S-CSCF or application server), assigning a S-CSCF to the UE and routing incoming requests further to an assigned S-CSCF or application server.

The Serving Call Session Control Function (S-CSCF) is the central node of the IMS as it is responsible for handling registration processes, making routing decisions and maintaining session states, and storing the service profile(s).

1.3 Common IMS

Since operators aim to provide services through many access networks, it is important to take the widespread issues of these different networks into account when designing a new platform. In the initiating phase of the IMS development, specifications where designed for the

different access networks by several standardization organisations. These specifications were not considering the integration of the different types of access networks, which is undesirable for the network operators providing the services.

Therefore, the standardization organisations have agreed to standardize Common IMS, which is the specification of the IMS architecture considering one operator serving multiple access networks. They decided to have the 3GPP develop the necessary specifications for Common IMS.

Implications for security are that there should be security mechanisms for every access network and in the case that there are multiple available security mechanisms for an access network the mechanism providing the highest security level should be activated. However, some security mechanisms should not work with every access network but only with the prescribed access networks.

1.4 Security in IMS

1.4.1 IMS Security overview

Since IMS is a service offering framework independent of the access network infrastructure, one should understand that 3GPP defines the standardized IMS solution as an overlay on top of the access domain. This architecture has consequences for the security model and should be considered when looking at the signalling and user traffic protection offered by IMS.

Access to IMS services requires authorization. This authorization is based on user authentication performed in conjunction with user registration in the IMS systems. The protocol used for user authorization is the IMS Authentication and Key Agreement (AKA) protocol [5] and is similar to the UMTS AKA procedure, hence providing mutual authentication. It also provides shared keys between the user and the IMS domain, which will be used for the protection of SIP signalling between the user endpoint and the P-CSCF of the user's IMS home network. Authentication and authorization is never been delegated to the visited network, but is always controlled by the home network's Authentication Centre (AUC).

Every IMS user is assigned a Private User Identity, which uniquely identifies the user's subscription and is authenticated at user registration. Associated with the Private User

Identity, one or more Public User Identities are allocated to the IMS user. These private and public user identities and algorithms for user authentication and registration are stored in an IP Multimedia Services Identity Module (ISIM), which is similar to a Subscriber Identity Module (SIM) or Universal Subscriber Identity Module (USIM) used in a UMTS access domain. This ISIM is an application on a Universal Integrated Circuit Card (UICC), which, in the cellular environment, resides next to the USIM and therefore having the same type of protection as the access domain credentials. The USIM holds access network credentials and algorithms, while the ISIM stores IMS network credentials and algorithms.

IMS user media traffic and IMS SIP signalling traffic are carried as user data in the access network. Since the security in the access network may vary and may not even be present, IMS traffic might not be integrity and confidentiality protected. To remedy this, IMS provides mandatory integrity and optional confidentiality protection of all SIP signalling messages between a user endpoint and a P-CSCF. The IMS AKA generated keys are used in the establishment of the necessary security associations. Security between the distinct interconnected IMS nodes and domains is provided by the Network Domain Security (NDS) standard [6].

1.4.2 Network Domain Security

In order to secure all IP traffic in the IMS core network, which 2G systems omit, 3GPP has specified the Network Domain Security standard [6]. It achieves this by providing confidentiality, data integrity, authentication and anti-replay protection for the traffic, using a combination of cryptographic security mechanisms and protocol security mechanism applied in IP security (IPsec).

The central concept of NDS is the security domain. A security domain is typically a network operated by a single administrative authority that maintains a uniform security policy within that domain. In many cases a security domain will correspond to an operator's core network. However, it is possible to have several security domains consisting out of a subset of the operator's entire core network.

Distinct domains are interconnected through the Za interface, which is mandatory to implement, while elements within a domain are interconnected through the optional Zb

interface. Data authentication and integrity protection is mandatory for both interfaces, while use of encryption is optional for Zb as being recommended for Za.

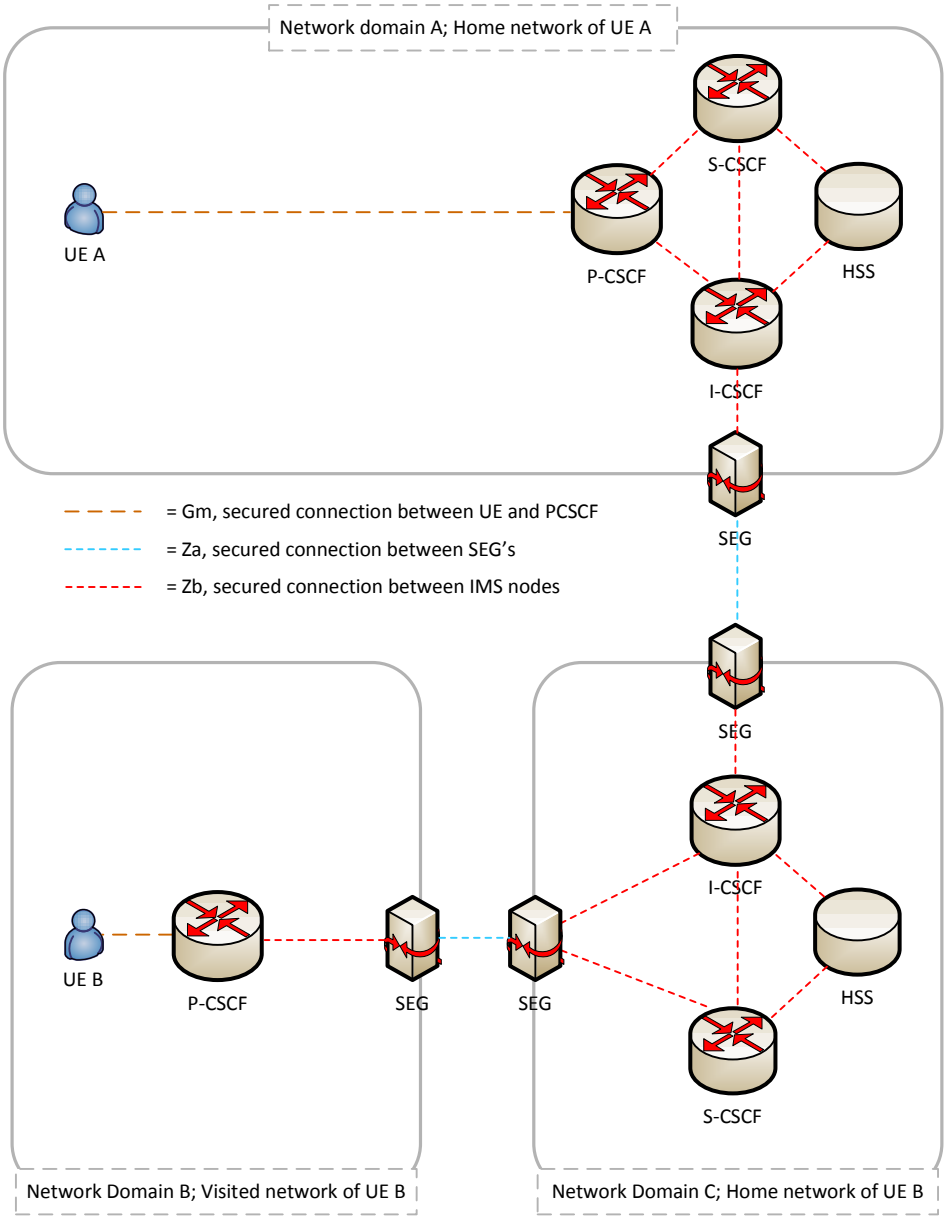

Figure 1.3 Network Domain Security in IMS

The concept of a home network and a visited network in which an IMS user endpoint can reside leads to basically two scenarios, depending on whether the IMS user is roaming or not. Figure 1.3 illustrates how these scenarios affect the concept of security domains.

Security gateways (SEG's) are entities located at the borders of security domains and are responsible for setting up and maintaining IPsec tunnels to peer SEG's. All traffic from a

network element in one security domain towards a network element in a different security domain is routed via a secure IPsec tunnel established between the SEG's. These SEG's implement the Za interface and apply Encapsulating Security Payload (ESP) [9] in tunnel mode to provide integrity and optional confidentiality protection. If network elements within a security domain implement Zb, ESP is applied as well. For both Za and Zb, the Internet Key Exchange (IKE) protocol [9] is used to negotiate, establish and maintain ESP Security Associations.

1.4.3 IMS access security

With NDS user traffic is secured within the IMS core network, but it does not provide security between user endpoint and its IMS access points, the P-CSCF. As stated before, IMS signalling and media data is the data payload for the access network and as such one should rely at the access network security mechanisms. However, access network operators are not obliged to offer data confidentiality and integrity and therefore IMS user data may be unprotected within the access network. Therefore IMS offers mandatory integrity and optional confidentiality protection.

Depending on the security mechanism chosen during the registration phase, two kinds of solutions can be used for integrity and confidentiality protection. One solution applies the IPsec ESP protocol, using the IMS AKA session keys for ESP Security Associations. The Integrity Key (IK) is used as authentication key and the Cipher Key (CP) as the encryption key. The second solution uses a TLS connection between user endpoint and P-CSCF.

1.4.3.1 Authentication and Authorization

To access services and to setup secure connections with the IMS core network the user endpoints perform the IMS AKA protocol [5]. This protocol is runned during initial registration performing mutual authentication between user endpoint and S-CSCF and is a challenge-response protocol. Figure 1.4 illustrates this IMS AKA authentication procedure.

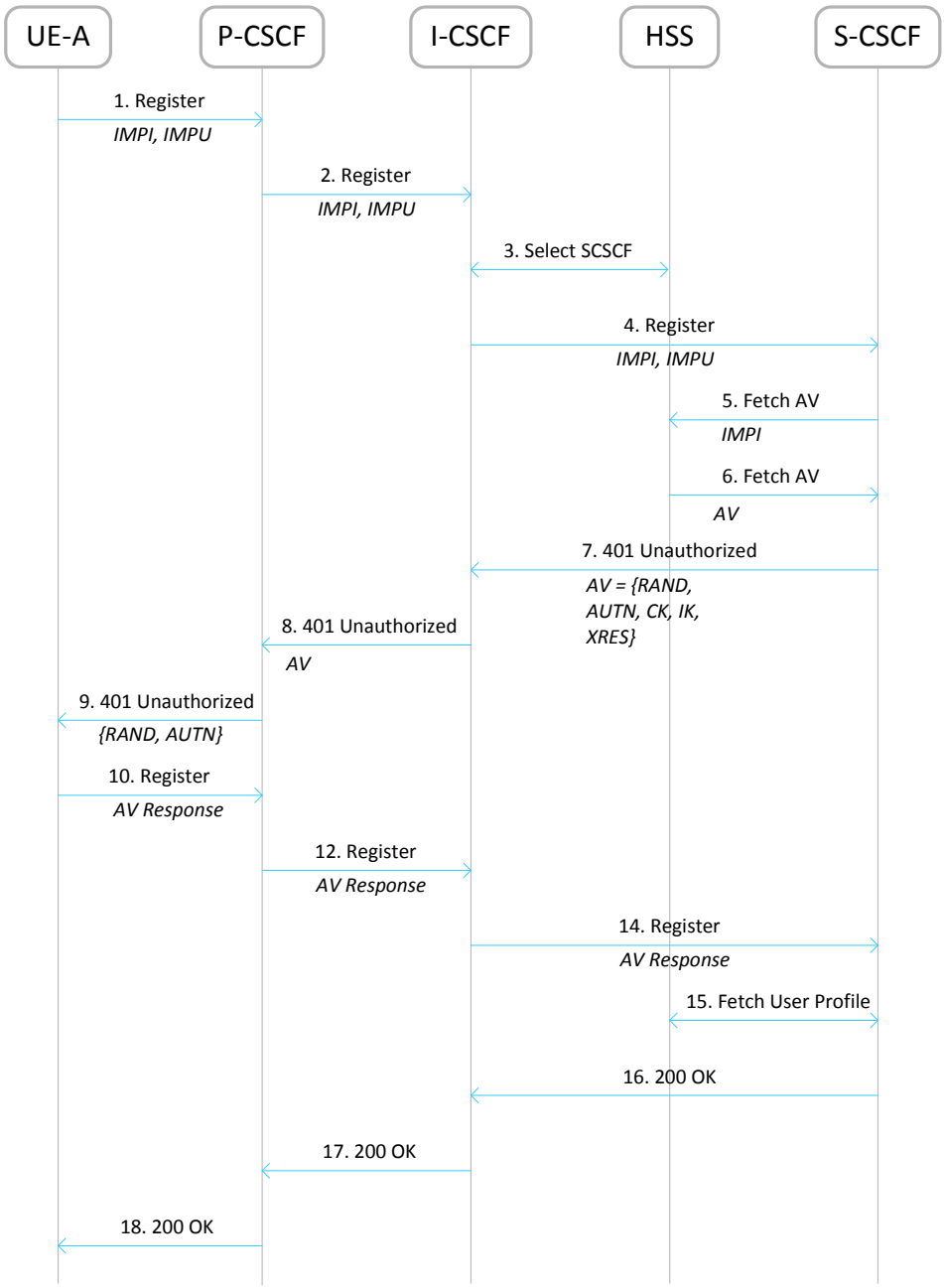

Figure 1.4 IMS AKA procedure

In the first steps the User Equipment sends a REGISTER request and indicates the Public User Identity (IMPU) and Private User Identity (IMPI) it wants to register. When this request reaches the I-CSCF the I-CSCF fetches the address of the correct S-CSCF from the Home Subscriber Server (HSS) and forwards the request to that S-CSCF. This server fetches an Authorization Vector (AV) from the HSS, containing an random challenge RAND, authentication token AUTN, cipher key CK, integrity key IK and the expected output for the challenge XRES. CK, IK, AUTN and the response RES can only be derived with knowledge of a key K, which is a shared secret

between HSS and User Equipment (mostly residing on an ISIM). The AV is sent back in a 401 Unauthorized message to the P-CSCF, which transforms the AV a little bit, so the UE only receives RAND and AUTN. Next the User Equipment verifies the AUTN which authenticates the network to the user and calculates the response RES and sends it in a new REGISTER request to the network. The S-CSCF compares the XRES with RES and authenticates and registers the User Equipment.

1.4.4 Media security in IMS

Currently, IMS security provides protection only for signalling messages and media security relies on underlying networks, cellular networks are assumed to provide sufficient media protection for instance. But since the access network may vary, security solutions may differ or may not even be provided. Therefore, 3GGP and others have started research for protecting media traffic on IMS level. Their requirements and proposed solutions are documented in [10] and will be discussed in chapter 2.

1.5 Open Source IMS Core

Worldwide many operators have currently IMS in trial phases and R&D departments are examining the possibilities of the framework. While there are already many open source projects with respect to VoIP and SIP, there is a almost no open source project with specific focus on the IMS. Therefore Fraunhofer Institute FOKUS has developed the Open Source IMS Core project, which aims to fill the currently existing IMS void in the open source software landscape.

Open Source IMS Core is based on SIP Express Router (SER) and is a flexible and extendable IMS solution enabling the development of IMS services and the trial of concepts around core IMS elements that are based upon highly configurable and extendable software. It is not intended to become or act as a product in a commercial context, but its sole purpose is to provide an IMS core reference implementation for IMS technology testing and IMS application prototyping for research purposes, typically performed in IMS test-beds. Therefore it can be used under the GPL license.

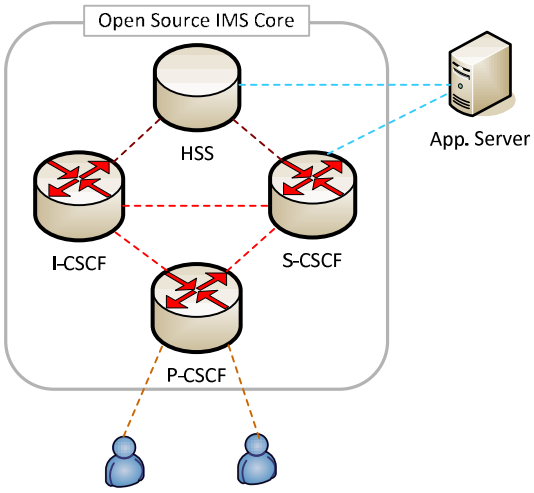

Figure 1.5 Architecture Open Source IMS Core

Figure 1.5 shows the architecture of the Open Source IMS Core system. It consists of several Call Session Control Functions (CSCF's), the central routing elements for any IMS signaling, and a Home Subscriber Server (HSS) to manage user profiles and associated routing rules. The central components of the Open Source IMS Core project are the Open IMS CSCF's (Proxy, Interrogating, and Serving) which were developed as extensions to the SIP Express Router (SER). But since even basic signaling routing functionality for IMS requires information look-up in a HSS, normal usage of such a core IMS network is not possible without it, therefore a simple HSS, the FOKUS Home Subscriber Server (FHoSS) is also part of the Open Source IMS Core project.

The Open Source IMS Core project is part of the Open IMS Playground, which is a technology focused test environment developed by FOKUS, where people can 'play' around with the latest technology. It is a mature testbed, where benchmarking, conformance tests and interoperability tests are carried out for FOKUS partners and where components resulting from FOKUS' own development can be deployed and operated.

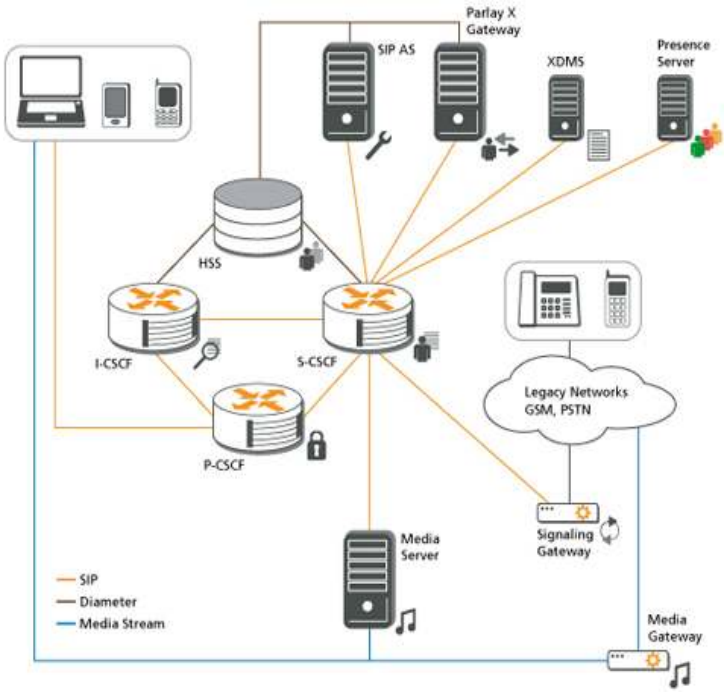

Figure 1.6 The Open Source IMS Core within the Open IMS Playground

1.6 Research questions

This thesis will focus on the research to solutions for setting up media path security in IMS. It will discuss which currently investigated solution fits best the stated 3GPP requirements and demonstrates an implementation in the FOKUS Open Source IMS Core environment. It compares the currently proposed solutions with regards to their fulfilment of the requirements and their impact on the IMS architecture. The main research question will be:

'Which solution for offering media security is most suitable for Open Source IMS Core considering the security requirements stated by 3GPP and considering the practical software engineering situation?'

Other related sub questions to which this thesis will try to find an answer include:

- Inventory of solutions
  - Which protocols may be used for media security?
  - Which key exchange protocols may be used?
  - What are the currently proposed solutions by other parties?
- Requirements analysis
  - What are the requirements for key exchange for IMS?

- Which requirements do the proposed solutions meet?
- Which solution matches the requirements best?

- Architectural consequences
  - What is the impact of the solutions to the Open Source IMS Core architecture?
  - Which solution is the best solution from architectural point of view?
- Selecting a solution
  - Considering the requirements analysis and the architectural consequences, which solution has the overall best results?
  - Which open source solutions are already available?
  - What are the practical boundaries and problems for implementing a solution?

The following chapters will discuss the related work and research considering media security (chapter 2), the method and models on which the results of this thesis are based (chapter 3), the results of the research (chapter 4), conclusions and discussions (chapter 5).

2 Related work and research

This chapter describes the related work regarding media security in IMS and in similar systems and it tries to address some of the subquestions listed in section 1.6. Section 2.1 describes related research done by the Internet Engineering Task Force (IETF). This is relevant since IMS is based on IETF protocols and some of the key exchange solutions are standardised by IETF. Section 2.2 describes the use-cases and requirements setup by 3GPP. Section 2.3 discusses the possible solutions, which have been examined by the IETF or 3GPP for IMS purposes and the solutions proposed by third parties.

2.1 IETF

The IETF is a large open international community concerned with the evolution of the internet architecture and the smooth operation of the internet. They examine and standardize internet protocols and for that reason they have standardized protocols for Voice over IP (VoIP) and media security in VoIP as well. The 3GPP used these IETF standardized protocols in order to facilitate its own IP Multimedia Subsystem, making it the 'access-independent, standard-based IP connectivity and service control architecture … using common Internet-based protocols' it is nowadays. Because of the use of these protocols, the IMS may have a similar architecture as some VoIP systems and may even be looked at as an applied VoIP system. Next sections describe media security in VoIP and its related protocols investigated by the IETF over the last few years; detailed technical descriptions of these protocols can be found in 23.

2.1.1 Voice over IP

Voice over IP is a technique which may be used in several different contexts and therefore the architecture of a VoIP system may differ from occasion to occasion. However, contexts in which a VoIP system uses a SIP server for setting up a VoIP connection between two endpoints have a similar global architecture as IMS, compare Figure 1.1 and Figure 2.1, which is due to the fact that IMS uses the same, already by the IETF standardized protocols and therefore based its architecture on these kinds of VoIP systems. The used standardized VoIP protocols include:

- the signalling protocol for session setup, the Session Initiation Protocol (SIP) [15]
- the Session Description Protocol (SDP) [16], which is used to negotiate session parameters

- the Real-time Transport Protocol (RTP) [18], which handles real-time transport of the media.

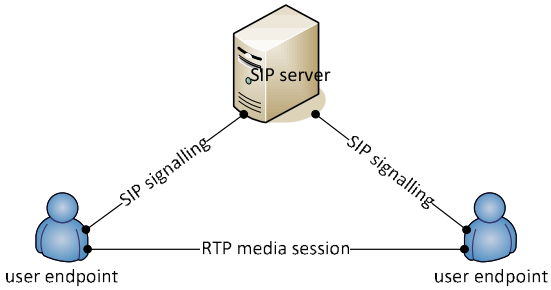

Figure 2.1 VoIP architecture using a SIP server

2.1.2 Media security in VoIP

The security workgroup of the IETF has investigated a few methods for setting up a secure media stream of a VoIP application. Regular well-known internet security protocols like TLS and IPSec cannot be used for this purpose, because the connection-oriented property of TLS and the large overhead of IPSec makes them unsuitable for real-time communication [14]. However, other solutions for encrypting the media path do already exist, but currently their main problem is the key exchange.

The protocol standardized for securing RTP is the Secure Real-time Transport Protocol (SRTP) [19]. This protocol provides payload encryption, message authentication, message integrity and replay protection and adds only a small amount of overhead to the RTP packet, becoming a lightweight protocol very suitable for securing real-time data. However, it assumes keys are already available and therefore a secure VoIP solution should also consist of a key exchange and key management protocol.

Another possibility for securing RTP data is the use of Datagram-TLS (DTLS) [13, 14]. This is a protocol similar to TLS, but designed for datagram transport protocols like UDP, instead of connection oriented ones like TCP. Therefore it offers the same security features as TLS, but because of its datagram transport capabilities it is well suited for securing delay sensitive applications. There are two main differences with SRTP:

- DTLS has its own key exchange mechanism which SRTP has not.

- DTLS wraps its own header and trailer around the RTP, making the whole packet length considerably larger. Figure 2.2 to Figure 2.4 illustrate the structure of RTP, SRTP and DTLS message, showing the relative overhead of DTLS compared to SRTP.

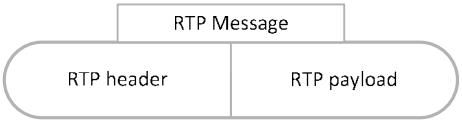

Figure 2.2 RTP message structure

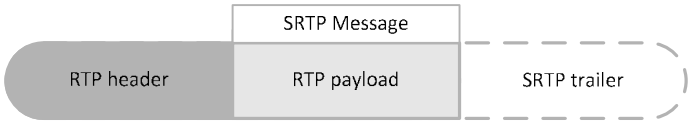

Figure 2.3 SRTP message structure: SRTP encrypts only the RTP payload and authenticates the RTP header and payload

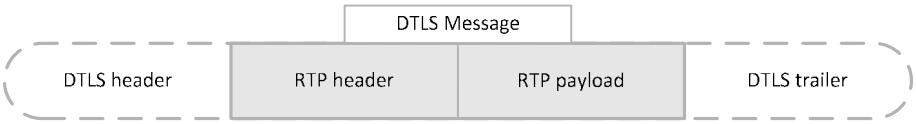

Figure 2.4 DTLS message structure: DTLS encrypts the whole RTP message and adds its own header and trailer

Because SRTP was specifically designed for RTP it has less overhead and is therefore more efficient than DTLS. This makes SRTP the preferred protocol to use in VoIP media security [23]. This also implies that a complete secure VoIP solution contains a key exchange protocol. Within the IETF there is still a discussion running about which key exchange protocol to use in a VoIP environment. The following section will elaborate on that topic.

2.1.3 Key exchange protocols

The IETF currently discusses three categories of key exchange protocols; one kind uses the signalling path for key exchange and the second uses the already setup media path. The third option combines both paths resulting in a hybrid key exchange solution. The first category includes protocols like SDES and MIKEY, ZRTP is a protocol using only the media path and DTLS-SRTP is a protocol which combines both the signalling as the media path.

2.1.3.1 SDES

SDES [17] is a standardized protocol specifically designed for SRTP usage. It stands for SDP Security Descriptions and is a way for negotiating SRTP keying material by use of an extra 'a=crypto' attribute within the SDP attachment of a SIP message. However, SDES is not able to generate keys itself; it depends on existing implemented protocols and algorithms in the VoIP system.

2.1.3.2 MIKEY

The alternative signalling path protocol, Multimedia Internet KEYing (MIKEY) [20], also adds an SDP attribute containing keying material, but it has several methods for exchanging this material:

- it can use pre-shared keys (PSK modus),
- it can exchange public keys using a public key infrastructure
- it can exchange keys using Diffie-Hellman algorithm.

However, there are some drawbacks using this protocol. The pre-shared key variant introduces the same problem SRTP already have: keys should already be available. The exchange of public keys may need a public key infrastructure, which may not desirable when an operator wants to roll out a commercial VoIP system. The Diffie-Hellman variant has a higher resource consumption than previous methods, but it may be a solid solution. However, MIKEY, in all its variants, is not in widespread use.

2.1.3.3 ZRTP

To avoid signalling path security dependencies Phil Zimmerman proposed the ZRTP protocol [21] for standardization to the IETF. ZRTP doesn't use the signalling path to transport keying material, but it uses the established unsecured media path to negotiate keys for end-to-end media security by means of Diffie-Hellman key agreement. After exchanging the Diffie-Hellman values keys are generated for the SRTP protocol and the media path becomes secured.

2.1.3.4 DTLS-SRTP

The hybrid solution is DTLS-SRTP [22], which uses the handshake of DTLS for key exchange and uses SRTP for RTP encryption. This method has the benefits of both DTLS and SRTP that it has a key exchange mechanism and that it has an as small as possible overhead. It creates a protocol with both efficient key exchange and efficient RTP security. The drawback is that it uses SDP to exchange the DTLS fingerprint, which is used to guarantee that no man-in-the-middle attack on

the certificates can be performed. By using SDP the fingerprint may be potentially exposed to eavesdroppers and therefore does it require signalling path security to verify the integrity of the SDP message. Keying material, however, is not exchanged over the signalling path.

2.1.3.5 Comparison & current status

The drawback of both SDES and MIKEY is that they transport keying material in plain text within the SDP attachment. The consequence of this fact is that the signalling path must be secured as well.
Signalling path security also applies for DTLS-SRTP, since the fingerprint in the SDP message should be integrity protected.

The IETF is still in discussion about which key exchange and management protocol to use for securing VoIP applications. [23] gives an insight about the currently state of the art in this discussion and handles the protocols into more detail.

2.2 3GPP

The 3rd Generation Partnership Project (3GPP) is the union of organizations initially aiming at developing technical specifications and technical reports for a 3G Mobile System based on evolved GSM core networks and the radio technologies that they support. IMS is developed by 3GPP and every part of the system is specified in a Technical Report. The 3GPP uses a system of parallel releases, to provide developers with a stable platform for implementation and to allow for the addition of new features required by the market. Currently they have frozen release 8 in December 2008, which has become a stable release and they are adding new features in release 9. Media security has been a study item since 2007 and a Technical Report will be created for the first time for release 9.

This section describes the use cases and the requirements for IMS media security specified by the 3GPP and the solutions they have already looked in to [10].

2.2.1 Use Cases

The 3GPP states that the protocols for the actual media plane protection are uncontroversial as the working assumption is to use well established protocols like SRTP [10]. This only leaves questions about how the key management solution should be designed and where the end-points for the media protection are located.

To setup requirements which cover all scenarios in which key exchange for media security may play a role, the 3GPP has defined multiple use cases considering the different purposes and varying relevance of IMS media security for different user groups. They distinguish three different purposes IMS media security may serve;

- protecting access media to establish a security level for IMS media over access networks which would be comparable with the access protection in cellular network;
- end-to-end protection for the vast majority of users, for which peer-to-peer voice calls will initially be the most significant use case and end-to-end protection is needed;
- enhanced end-to-end protection to provide security measures for user groups with well-defined security requirements, e.g. enterprises, government authorities.

The described use cases can be divided according to the scenarios they apply to and the 3GPP distinguishes the following scenarios in which media security plays a role:

- *Multimedia telephony;* This scenario is divided into several subscenarios in which end-to-end media security is a requirement.
    - *Peer-to-Peer;* this is the most common use case and describes a call from one peer to another. Except the usually directly established call between initiating and receiving terminals, it also makes notice of forwarding of the call to another user's terminal and forking of the call, which means that the call is initially directed to more than one terminal. The most important considerations in this use case is that only the party picking up the call should get access to the plaintext media. Considerations about picking up more than one terminal are discussed in the group and conference call use case.
    - *Non RTP based media;* A multimedia telephony session may include non-RTP based media like file transfer, video clip sharing, etc. Such media is normally MIME encoded and transported over the Message Session Relay Protocol (MSRP) [25][26] and may be protected by (PSK)TLS [27][28] or using S/MIME [29].
    - *Deferred delivery;* This use case describes the case when a call ends up in a voice or other media mail box in the network. Preferably the media is stored in its encrypted format and is not decrypted before storing and encrypted again when sending to the receiver. The consequence for key exchange is that a key management system is required which does not depend on the identity of

transmission end-points but on the identity of the sender and receiver. Therefore it may require new media set-up signalling mechanisms and new media protection mechanisms or a combination of existing ones.

- *Group and conference calls;* This use case describes secure media sessions between multiple users, the so-called conference calls, with end-to-end security. In this type of service it is necessary that all users have access to the same key.

Considering these several subscenarios a key management system should in addition to straightforward point-to-point channel protection, support group keying, application layer security (security independent of the transport mechanism) and deferred delivery of end-to-end protected media.

- *Push-to-talk (PoC);* A push-to-talk system is able to store and forward messages to multiple users. It is able to handle other media types than voice as well. This implies the same characteristics and therefore the same requirements on key management and media protection as multimedia telephony.
- *Instant messaging;* Instant messaging (IM) systems have many similarities with PoC systems, the main difference is that they focus on non-speech media even though they may also carry voice and video messages.
- *Chat;* This use case differs from IM, because the chat messages usually end up in the chat server where they are handled in plaintext. End-to-end security means in this case security from endpoint to chatserver and the communication between endpoint and server requires the same type of protection of media as used to protect IM.
- *Transcoders;* Transcoders are devices in the network that need to change or modify the media streams. Therefore media protection needs to be terminated at the transcoder.
- *PSTN-GW;* PSTN gateways provides interworking between IMS networks and circuit switched PSTN and is the final node within the IMS network. Therefore media protection needs to be terminated in the PSTN-GW.
- *Termination of media security in an Application Server;* An IMS session is not always setup between two user endpoints. It may also be terminated in an Application Server (AS). Therefore media protection should be terminated at the AS.

2.2.2 Requirements

This section gives an overview of the requirements for IMS media security stated by the 3GPP in [10]. They have categorised the requirements into the following eight different categories:

- Lawful interception
- Security
- Requirements related to SIP based call features/SIP related problems
- Architectural
- Scalability, Cost and Performance
- Requirements regarding the access network type
- Backward compatibility and migration
- Other requirements

Within some categories the 3GPP distinguish their own 3GPP requirements and standard internet requirements defined by the IETF. The following tables show the requirements per category, where the identifier has a direct link to the corresponding requirement within [10] and shows whether it is a 3GPP or IETF formulated requirement. In the category 'other requirements' requirements may occur which are already mentioned in earlier categories, but they are deliberately included, because they correspond to the requirements mentioned in [10].

Lawful Interception	
ID	Description
3gpp.1	Lawful interception shall be met.
3gpp.2	The lawful interception solution shall not require the operator to reveal information to the interception agent that would allow him to intercept user communication that are outside the terms of the intercept warrant.
3gpp.3	It shall not be possible for users to detect whether or not their communication is subject to lawful interception.

Table 2.1 Lawful interception requirements

Security	
ID	Description
3gpp.4	It shall be possible to protect IMS user traffic against eavesdropping, modification, spoofing and replay on access network interfaces and access network nodes.

3gpp.5	It should be possible to protect IMS user traffic against eavesdropping, modification, spoofing and replay on core network interfaces and at core network nodes. Depending on the use case, this protection shall be equal or higher than the protection for IMS signalling traffic.
3gpp.6	The level of security provided should satisfy operators and the vast majority of users, whilst at the same time satisfying applicable interception requirements. An enhanced solution may additionally be provided if this level of security is insufficient for high security user groups.
3gpp.7	A key management solution shall be based on user identity (i.e. IMPI/IMPU).
ietf.8	A solution must provide protection against passive attacks.
ietf.9	A solution should consider active attacks.
ietf.10	A solution must be able to support Perfect Forwarding Secrecy.
ietf.11	A solution must support algorithm negotiation without incurring per-algorithm computational expense.
ietf.12	A solution must support multiple cipher suites without additional computational expense.

Table 2.2 Security requirements

Requirements related to SIP based call features/SIP related problems	
ID	Description
ietf.13	Forking and retargeting must work with all endpoints being SRTP.
ietf.14	Forking and retargeting must allow establishing SRTP or RTP with a mixture of SRTP- and RTP-capable targets.
ietf.15	With forking, only the entity to which the call is finally established, must get hold of the media encryption keys.
ietf.16	A solution should allow to start with RTP and then upgrade to SRTP.
ietf.17	Endpoint identification when forking; the offerer must be able to associate an answer with the appropriate endpoint.
ietf.18	A solution should avoid clipping media before receiving the SDP answer, without additional signalling.
3gpp.19	A key management solution shall support secure multiparty communications where the server relaying multiparty communication does not know the group key.
3gpp.20	A key management solution shall support secure multiparty communications where

	the server relaying multiparty communications knows the group key.

Table 2.3 Requirements related to SIP based call features/SIP related problems (Forking and Retargeting, Early media/media clipping, Secure multiparty communications)

Architectural	
ID	Description
3gpp.21	Encryption and integrity protection of user media should be applied on an end-to-end basis, where possible, to save on network resources and to avoid restrictions on media plane routing.
3gpp.22	Where it is not possible to provide protection on an end-to-end basis due to cost or complexity reasons, then solutions should be developed which terminate user plane security in an appropriate network element.
3gpp.23	It should be possible for operators to be able to terminate media plane security in the network in some cases, e.g. if the operator needs access to the media for content control purposes.
3gpp.24	A solution should support media recording.
3gpp.25	Multiple solutions should be avoided to reduce complexity in the network and to maximise interoperability between user devices. However, in case it turns out that there is no single solution satisfying all these requirements, or that a solution leads to undue complexity or delay, it may be acceptable to standardise more than one solution.
3gpp.26	The requirement for new functions on the user's smartcard should be avoided unless it would provide significant and cost effective benefits.
3gpp.27	The solution should support the possibility to protect user traffic on an end-to-end basis between IMS-capable user equipment and user equipment which is non IMS-capable.
3gpp.28	The solution shall have minimal impacts on already deployed network entities.
3gpp.29	A media security solution shall assume that messages cannot be sent over the media path until the media session has been established.
3gpp.30	A media security solution shall assume that only media traffic can be sent over the media path.
3gpp.31	Media security solutions for media protection and key management shall cover both end-to-end and end-to-middle media protection scenarios.

ietf.32	A solution must not require 3rd-party certificates. If two parties share an auth infrastructure they should be able to use it.
ietf.33	From an architectural point of view solutions can exchange key exchange messages along the media path, along the signalling path or on both paths. A solution should operate along the media path and the signalling path. *Comment: In the 3GPP architecture the preferred solution is to perform the key exchange messages in the signalling path only.*

Table 2.4 Architectural requirements

Scalability, Cost and Performance	
ID	Description
3gpp.34	The solution should scale well for large numbers of users.
3gpp.35	The solution should be cost effective.
3gpp.36	The solution should not adversely affect performance of IMS services. In particular, there should be no significant increase in call set-up delay and no media clipping.

Table 2.5 Scalability, Cost and Performance requirements

Requirements regarding the access network type	
ID	Description
3gpp.37	The solution shall support the possibility to provide protection on an end-to-end basis between any IMS-capable user endpoint regardless of what type of access technology they use (fixed DSL, WLAN, cellular, etc).
3gpp.38	The key management solution should be based on the existing IMS access security architecture, so that no special user registration or user involvement is required and so that existing infrastructure can be re-used.
3gpp.39	Since the IMS client may use different access authentication methods, the key management solution for end-to-end security shall be able to work independently of any of these authentication methods.

Table 2.6 Requirements regarding the access network type

Backward compatibility and Migration	
ID	Description
3gpp.40	Media security shall be mandatory to implement for user endpoints and networks and optional to use for user endpoints.

3gpp.41	The media security solution shall allow a user endpoint to negotiate media security settings for each individual call.
3gpp.42	The negotiation of media security must be protected against downgrading attacks.
ietf.43	A solution must allow a SIP user endpoint to negotiate media security parameters for each individual session.

Table 2.7 Backward compatibility and Migration requirements

Other requirements	
ID	Description
3gpp.44	A solution shall support the possibility to protect RTP-based IMS user plane traffic.
3gpp.45	A solution shall support the possibility to protect non RTP-based IMS user plane traffic. If a single solution leads to undue complexity or delay in standardisation or deployment it may be acceptable to standardise more than one solution. If multiple solutions are standardised, then they shall be defined within a single framework.
3gpp.46	A solution shall support the possibility to protect application layer messages, e.g. SIP MESSAGE.
3gpp.47	The media security solution should not require user intervention.
3gpp.48	A party shall have the possibility to get assurance about the identity of any other party in the session when the party joins a point-to-point session.
3gpp.49	A calling party shall have the possibility to stay anonymous towards any called parties in the session.
3gpp.50	The user should be able to access information about the scope of protection (end-to-access edge, end-to-middle or end-to-end) and applied security level. It should also be visible if any non-IMS operators are involved in the session.
3gpp.51	It should be possible to configure the terminal to give a visible or audible warning when security is not according to a user defined policy.
3gpp.52	A key management solution shall support deferred delivery of media. If a single solution also supporting deferred delivery leads to undue complexity or delay in standardisation or deployment it may be acceptable to standardise more than one solution. If multiple solutions are standardised, then they shall be defined within a single framework
ietf.53	A solution should support the possibility to protect non-RTP based data traffic.

Table 2.8 Other requirements

2.3 Proposed solutions

This section presents a summary of the candidate solutions for enabling media security in IMS proposed by the 3GPP, which are extensively described in [10], and by other parties.

2.3.1 Ticket-Based System

The Ticket-Based System (TBS) is a framework in which requirements from different user groups can be accommodated. A 'ticket' concept, similar to Kerberos, is used to identify and deliver keys. 3GPP describes the delivery of keys with MIKEY as key exchange protocol, which is discussed in section 2.1.3.2 as key exchange protocol.

There are two categories of tickets: protected and unprotected. Using the unprotected tickets requires that the security of the complete IMS infrastructure must be trusted and in general, for normal customers this should be the case. Protected tickets may be used to achieve higher security and will provide security independent of the security of the IMS infrastructure, but in this case a Kerberos-like Key Management Server (KMS) must be trusted. Protected tickets will likely be required by enterprise users and national authorities and public safety organizations, who have limited trust in the IMS infrastructure and require high quality end-to-end media security.

In a TBS the sender requests a ticket from the key management service and sends the ticket containing the enveloped key or a reference to the key, to the receiver. The receiver then sends the ticket tot the key management service which then returns the appropriate key. Figure 2.5 illustrates this process. A precondition for this method is that the users can establish secure connections to the KMS and that mutual authentication is provided. In an IMS environment this can be achieved by the use of the Generic Bootstrap Architecture (GBA) [7].

Figure 4.1 illustrates the general architecture of a TBS using a key management server and paragraph 4.2.1 analyzes the architectural impact and consequences of this solution. As the figure makes clear fetching the key only depends on possession of the ticket T, which implies that the underlying connections between User Endpoints, Key Management Server and the IMS Network must be secured, so that eavesdroppers will not be able to intercept the ticket and fetch the master key.

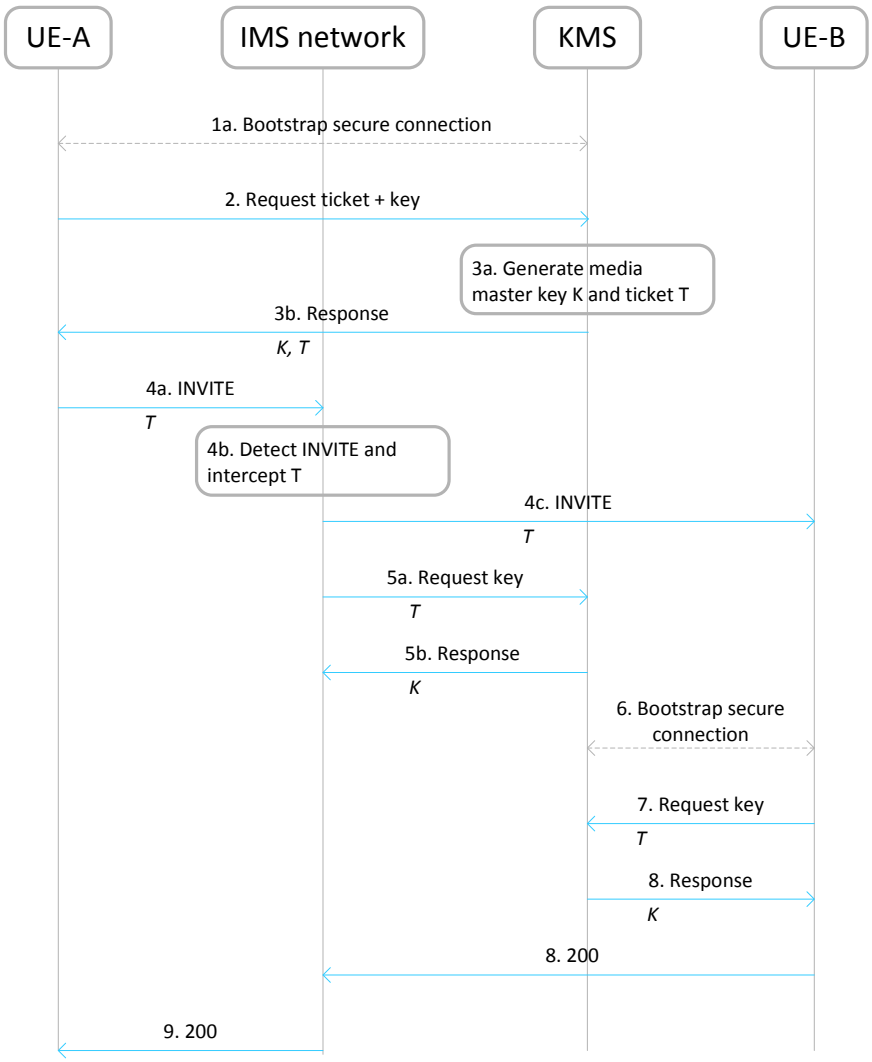

Figure 2.5 Ticket-Based key management system

2.3.2 Otway-Rees

Otway-Rees is a solution which also includes a Key Management Server and which is therefore architecturally very similar to the Ticket-Based System. Both users need to bootstrap through GBA with the KMS to establish both a shared secret 'Ka'/'Kb' with KMS. This shared secret is later on used to authenticate the users to the KMS when requesting the master key for media security and to encrypt the master key by the KMS when sending it to the users. Figure 4.2 shows the architecture of the Otway-Rees solution and Figure 2.6 illustrates the working of the protocol.

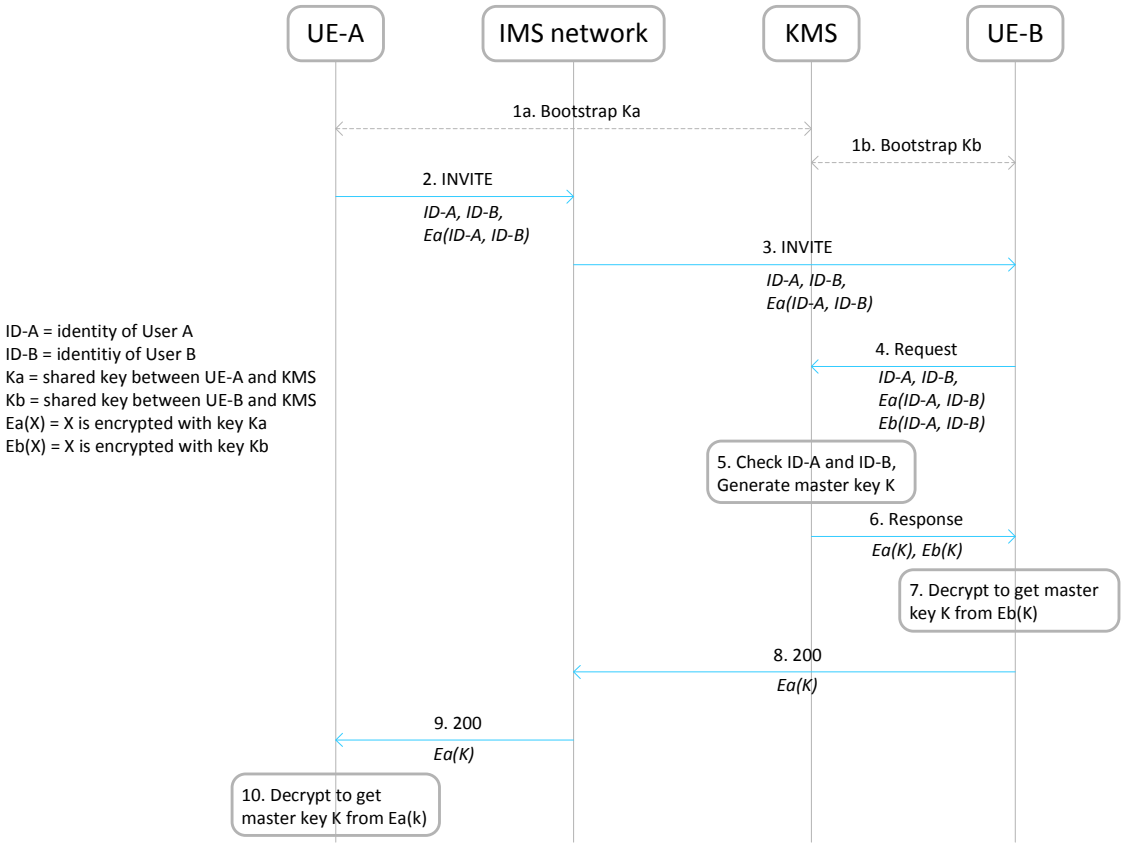

Figure 2.6 Otway-Rees key management system

2.3.3 SDES

SDES is already explained in section 2.1.3.1 and its application into IMS is very straightforward. When two users, A and B, establish a media session through IMS, user A includes the key, which encrypts the data sent from A to B, in its SIP INVITE message and user B includes a second key, which encrypts the data sent from B to A, in its SIP response message. The keys are put in plaintext in the SDP body of the SIP message and therefore the SIP messages have to be protected in order to prevent eavesdroppers from retrieving the keys.

In order to provide SDES to the users, adjustments have to be made to the user clients, IMS functions do not need to be altered. Even when network nodes need access to the media security keys they can just look into the SIP messages, since these are hop-by-hop protected and can therefore be accessed by the network nodes.

2.3.4 IMSKAAP

The Taiwanese researchers Chen et al. [12] have recently proposed and published an alternative key agreement authentication protocol for IMS (IMSKAAP) to achieve end-to-end

security for IMS user endpoints. They assume an architecture performing key exchange in the signalling path (using SIP and SDP) to establish an RTP session upgrading to SRTP. This section will summarize its design goals and the protocol mechanism.

2.3.4.1 IMSKAAP design goals

The IMS key agreement authentication protocol is based on the four-party key agreement authentication protocol (KAAP) proposed by Yeh and Sun [24] and the requirements are based on the 3GPP specification. However, Chen et al. have focused on a few specific items and therefore IMSKAAP is designed with the following five points in mind:

1. provide user identity privacy.
2. avoid client side PKI to obtain minimal user time and computing power.
3. cost reduction of delivering messages during key exchange by using SDP extension fields.
4. mutual authentication to ensure user/provider validity.
5. provide lawful interception.

2.3.4.2 IMSKAAP mechanism

The IMSKAAP is a Diffie-Hellman (DH) based protocol, in which two nodes do not exchange values with each other directly, but in which the users interact with their corresponding S-CSCF server in between. This results in two parties each consisting of a user endpoint and a S-CSCF server, in which both parties negotiate the DH values and where the user endpoint and its S-CSCF server both have the disposal of the same data.
Figure 2.7 shows the IMSKAAP procedure, which consists out of 8 message exchanges resulting in two roundtrips. An in-depth explanation of the image and a detailed description of the protocol can be found in [12].

In order to provide this protocol, the S-CSCF servers need to be adjusted with extra functionality. The IMSKAAP messages should be exchanged using SDP extensions, as defined in RFC 4567 and should be fitted within the session initiation procedure. This means that the S-CSCF servers should be able to detect the SDP attributes, to do some extra calculation and to alter some of the SDP attributes.

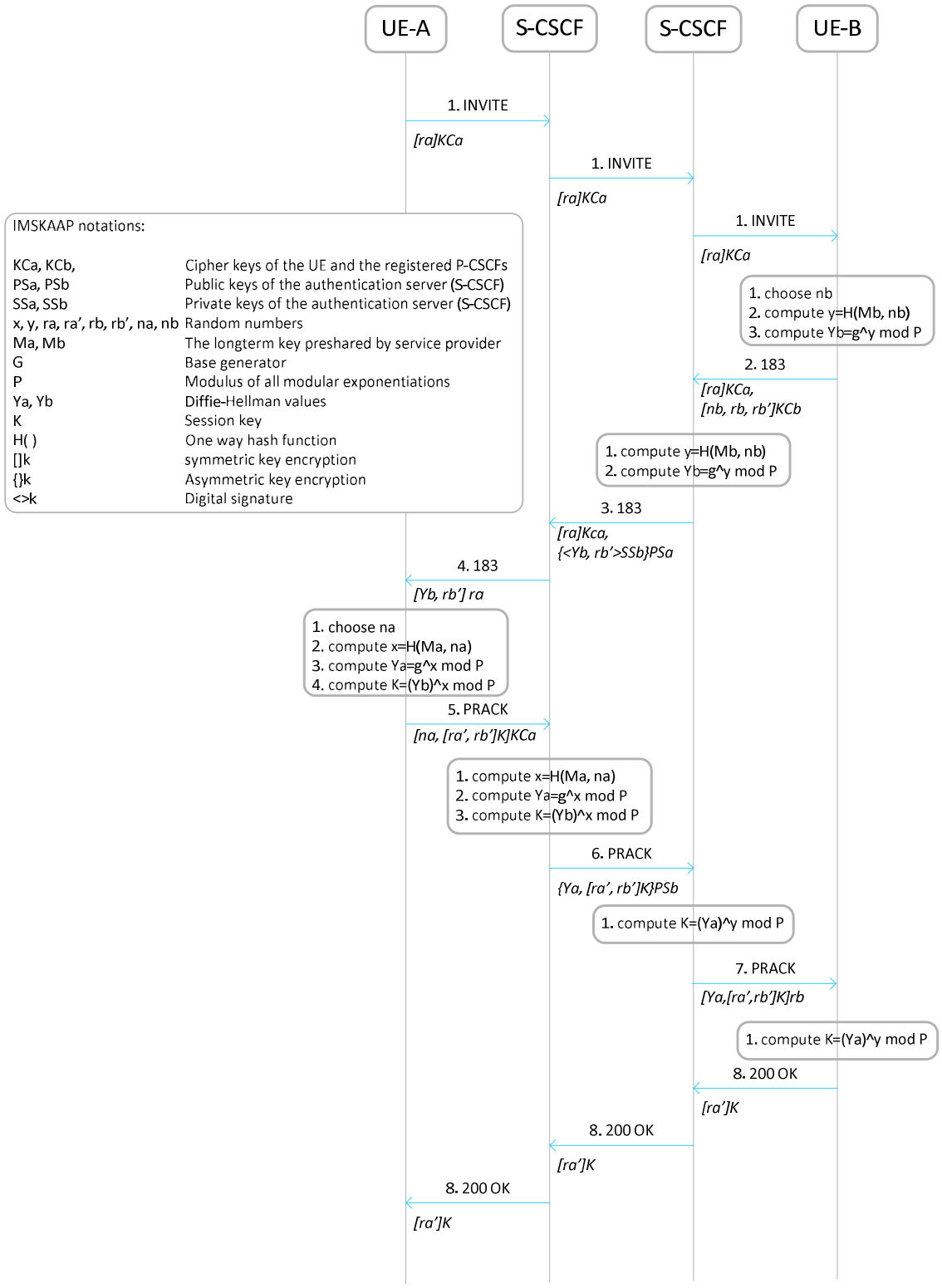

Figure 2.7 IMSKAAP protocol

2.3.5 DTLS-SRTP

DTLS-SRTP is a protocol developed by the IETF and the concept of it has already been discussed in section 2.1.3.4. It is an efficient protocol with small overhead and therefore seems very suitable for usage within VoIP systems in general and IMS in specific. However, the 3GPP has not discussed this protocol in its technical specification of media security in IMS yet, but since recently sounds have gone up in favour of this protocol and its predicted fitness the protocol should to be taken into account as a possible media security solution.

Since this protocol mixes control traffic (key management) and media traffic (protected payload), implementation of this protocol has some architectural impacts to IMS nodes:

- Additional resources than negotiated should be available to ensure that the DTLS handshake can be performed.
- Changes should be made to media related functions in order to handle DTLS-SRTP traffic to be passed through.
- In an inter-operator scenario, with the possibility of roaming, all operators and interconnect networks would have to make trade-offs, such as pre-open gates in gateways and media controlling nodes or commitment of resources.

2.3.6 Zfone-like applications

Other solutions for media security may include solutions like Zfone [30]. Zfone is an application to secure VoIP connections and is created by PGP-creator Phil Zimmerman and uses the ZRTP protocol [21]. This protocol establishes an SRTP connection using the RTP media path to exchange keying material and is therefore completely client based.

With respect to IMS, users can establish a normal media session using IMS signalling. When this session is established the users may choose to perform a Zfone-like application, which exchanges keying material over the media path and upgrades the RTP session to SRTP. It uses the same ports as RTP, so new resources do not have to be available. However, the protocols messages are different from RTP messages and therefore changes should be made to media related functions in order to handle ZRTP traffic to be passed through.

A solution like Zfone has little influence on the IMS architecture, since it is all client based and therefore only the IMS elements handling media traffic, e.g. media gateways, have to be altered in order to handle ZRTP traffic.

3 Research Setup

This chapter describes how the research is set up and what methods will be used for acquiring the results.

3.1 Solution comparison

The solutions described in previous chapter will be compared based on two different perspectives: a requirement point of view and an architectural point of view.

3.1.1 Requirements

The requirement analysis checks to which 3gpp requirements the solutions adhere to and the results of this analysis provide an overview of which requirements the solutions meet and how they meet them. Next a comparison between the different solutions will be made based upon the requirements they adhere to and a prioritization of the solutions will be made based upon this comparison. The comparison shows the differences and similarities between the different solutions regarding the requirements they meet.

3.1.2 Architecture

The architectural analysis illustrates the impact of the solutions to the current Open IMS Core architecture. An updated architecture for every single solution will be presented and a comparison, showing the differences and similarities between these architectures will lead to a prioritized list of architectural solutions.

3.2 Solution selection

After comparing the solutions at two different levels, the solution shall be prioritized based on the requirements and architectural analysis. The selection will point out the solution which is most suitable for implementing in Open Source IMS Core. For implementing practical environmental boundaries and time constraints will be taken into account.

3.3 Proof of Concept

One of the solutions will be (partially) implemented in Open Source IMS Core as a Proof of Concept to show that media security and lawful interception requirements coincide and to illustrate the issues regarding Open Source IMS Core in a practical environment. Results and

practical problems encountered during this phase will be discussed. The next sections already describe the setup of the system and other practical environmental parameters.

3.3.1 Hardware configuration

Hardware configuration of the development computer/Open IMS Core server:

Processor 0: Intel Core 2 Duo E8400 @ 3.00GHz

Processor 1: Intel Core 2 Duo E8400 @ 3.00GHz

Memory: 4 GiB DDR2 SDRAM

Harddisk: 160 GiB Hitachi Dekstar 7K160

Network: Intel 82566DM- 2 Gigabit

Operating System:

Ubuntu Release 8.04 (hardy)

Kernel Linux 2.6.24-12-generic

GNOME 2.22.3

3.3.2 Software installations

Open IMS Core is freshly installed following the install guidelines on the Open IMS Core website (http://www.openimscore.org/installation_guide). After installing the system, it was configured using the configurator.sh script to allow network access from other computers as well. One of the IMS client was running on the previous mentioned development system as well, the second client was running on a normal Microsoft Windows computer.

The clients used for this project are the C based, open source UCT IMS Client (http://uctimsclient.berlios.de/), which is designed to be used in conjunction with Fraunhofer Open Source IMS Core.

4 Results

This chapter describes the results of the requirement analysis and the architectural analysis with respect to Open Source IMS Core and describes the Proof of Concept and the .

4.1 Requirement analysis

This section shows per category from section 2.2.2 whether or not the solutions meet the 3gpp requirements and motivates the results when there are differences between the solutions or when the results are not trivial. The results are presented in tabular form and may be marked

- OK: the solution meets the requirement;
- OK*: the solution meets/fails the requirement depending on additional assumptions;
- NOK: the solution fails the requirement.

4.1.1 Lawful Interception

Lawful Interception						
ID	TBS	SDES	Otway-Rees	IMSKAAP	DTLS-SRTP	Zfone
3gpp.1	OK	OK	OK	OK	NOK	NOK
3gpp.2	OK	OK	OK	OK	OK	OK
3gpp.3	OK	OK	OK	OK	OK	OK

Table 4.1 Analysis of the Lawful Interception requirements

3ggp.1: *Lawful interception shall be met*

The DTLS-SRTP solution has major issues regarding offering lawful interception functionality, since no keying material passes network entities and therefore the network is not able to decrypt the encrypted media stream. However, network operators have already proposed some solutions from this problem to the 3GPP, but only the Key Disclosure variant seems feasible for implementation. This method describes that operators may demand user agents to send the key to trusted network nodes for every call by means of the subscription contract and discard all call attempts which do not comply to this procedure. The largest drawback of this solution is that cheating by the user, by means of disclosing a wrong key, is very difficult to prevent.

Another method for lawful interception functionality regarding DTLS-SRTP is the lawful Man-in-the-Middle attack. This requires all traffic to go through a network node on which such an

attack can be performed, since otherwise the attack can easily be detected by comparing the certificate fingerprint received during the DTLS-SRTP handshake by spoken voice. However, this method is a considerable effort to implement, brings higher costs and may impact the network enormously, demanding high performance network nodes.

Since Zfone is established through the media path only and therefore key material is not available to the IMS network entities, lawful interception is very hard to perform. A plain lawful Man-in-the-Middle attack as proposed for DTLS-SRTP is not an option here as well, since Zfone provides the Short Authentication String (SAS), which should be read aloud by the end users, and which ensures that no MitM attack has taken place even if all traffic goes through one network node. However, the ZRTP protocol used by Zfone offers the possibility for scenarios with a trusted-MitM, which is intended for users behind a PBX (Private Branch Exchange) and to which they are registered. This concept may be adjusted for IMS usage by pretending the IMS platform to be the PBX, enabling the possibility for a trusted-MitM. However, this requires the IMS operators to route all the media traffic through an IMS node in order to provide the lawful interception functionality, which brings higher implementation cost and considerably more effort and demands high performance IMS nodes for processing and routing all the traffic.

3gpp.2: *The lawful interception solution shall not require the operator to reveal information to the interception agent that would allow him to intercept user communication that are outside the terms of the intercept warrant*

In case of each alternative, tickets or keys are per session and therefore revealing the key for lawful interception will not reveal information with which communications that are outside the terms of the intercept warrant can be intercepted.

3gpp.3: *It shall not be possible for users to detect whether or not their communication is subject to lawful interception*

Every solution meets this requirement.

4.1.2 Security

Security						
ID	TBS	SDES	Otway-Rees	IMSKAAP	DTLS-SRTP	Zfone
3gpp.4	OK	OK	OK	OK	OK	OK
3gpp.5	OK	OK	OK	OK	OK	OK
3gpp.6	OK	OK	OK	OK	NOK	NOK
3gpp.7	OK	OK	OK	OK	OK	OK

Table 4.2 Analysis of the Security requirements

3gpp.4: *It shall be possible to protect IMS user traffic against eavesdropping, modification, spoofing and replay on access network interfaces and access network nodes*

If signalling protection is provided this requirement holds for every solution.

3gpp.5: *It shall be possible to protect IMS user traffic against eavesdropping, modification, spoofing and replay on core network interfaces and core network nodes*

If signalling protection is provided this requirement holds for every solution.

3gpp.6: *The level of security provided should satisfy operators and the vast majority of users, whilst at the same time satisfying applicable interception requirements*

This requirement can only hold if users and operators judge it by checking the solution to their own security requirements and if lawful interception can still be performed. In general each of these solutions offer sufficient security to the users. However, for DTLS-SRTP and Zfone, lawful interception functionality is difficult to fulfil.

3gpp.7: *A key management solution shall be based on user identity*

The TBS keys can only be used by authorized users, while in IMSKAAP the keys can only be created by authorized users and keys are also associated with user-ids.

SDES and DTLS-SRTP need signalling integrity and assertion of identities so a caller knows who he is talking to. If the call is answered by an undesired callee the caller can decide to cancel the call. However, this is not a protocol specific property and concerns all of the proposed solutions.

In Zfone, users have already established a media session before the key management protocol will execute. Therefore the identity of the users is already known to the key management protocol.

4.1.3 SIP based call features/SIP related problems

Requirements related to SIP based call features/SIP related problems						
ID	TBS	SDES	Otway-Rees	IMSKAAP	DTLS-SRTP	Zfone
3gpp.19	OK	NOK	OK	NOK	OK	NOK
3gpp.20	OK	OK	OK	NOK	OK	NOK

Table 4.3 Analysis of the requirements related to SIP based call features/SIP related problems (Forking and Retargeting, Early media/media clipping, Secure multiparty communications)

3gpp.19/3gpp.20: *A key management solution shall support secure multiparty communications where the server relaying multiparty communication does/does not know the group key*

The TBS can send the same key to several receivers and the content of the ticket can be made inaccessible to the controlling function of the server, but the server can also be authorized to access the content of the ticket, thereby meeting both requirements.

Users can send the same SDES keys to multiple users, but SDES cannot ensure that the controlling function of the server does not know the key, therefore only **3gpp.20** can be met.

Otway-Rees can send the same keys to multiple users and it is possible to encrypt the keys by the KMS using separate user specific keys.

When using IMSKAAP it is not possible to establish multiparty communications and to keep the servers from knowing the keys. IMSKAAP is designed to establish end-to-end security for two users, in which the servers compute the same keys as well.

DTLS-SRTP can be used for secure multiparty communication and it is able to ensure that the controlling function of the server does not know the key by using a key transport extension [31], which allows a peer, or a conference bridge, to dictate the SRTP master key.

Zfone is not able to establish secure multiparty communication and therefore these requirements cannot be met.

4.1.4 Architectural

Architectural						
ID	TBS	SDES	Otway-Rees	IMSKAAP	DTLS-SRTP	Zfone
3gpp.21	OK	OK	OK	OK	OK	OK
3gpp.22	OK	OK	OK	OK	OK	OK
3gpp.23	OK	OK	OK	OK	NOK	NOK
3gpp.24	OK	OK*	OK	OK*	OK*	OK*
3gpp.25	OK*	NOK	OK*	NOK	NOK	NOK
3gpp.26	OK	OK	OK	OK	OK	OK
3gpp.27	NOK	OK	NOK	NOK	OK	OK
3gpp.28	NOK	OK	NOK	OK	OK	OK
3gpp.29	OK	OK	OK	OK	OK	OK
3gpp.30	OK	OK	OK	OK	NOK	NOK
3gpp.31	OK	OK	OK	OK	OK	OK

Table 4.4 Analysis of the Architectural requirements

3gpp.21: *Encryption and integrity protection of user media should be applied on an end-to-end basis where possible, to save on network resources and to avoid restrictions on media plane routing*

Every solution is able to setup end-to-end security.

3gpp.22: *Where it is not possible to provide protection on an end-to-end basis due to cost or complexity reasons, then solutions should be developed which terminate user plane security in an appropriate network element*

Every solution is able to setup media plane security which terminates in an appropriate network element.

3gpp.23: *It should be possible for operators to be able to terminate media plane security in the network in some cases, e.g. if the operator needs access to the media for content control purposes*

Since network elements can be authorized to fetch the keys this requirement is no problem for solutions like TBS, Otway-Rees and SDES. IMSKAAP has no troubles as well, since user nodes and the network elements exchange information with which they compute the same keys.

DTLS-SRTP can only satisfy this requirement when key disclosure is supported, but as already discussed, key disclosure is most likely not feasible due to customer behaviour.
Zfone is only able to satisfy this requirement in combination with the trusted-MitM. The back-to-back middlebox captures every call and does ZRTP negotiation, so it can encrypt and decrypt traffic coming in and going out.

3ggp.24: *A solution should support media recording*
This requirement is still being studied by the 3GPP in order to define it properly, since it does not state whether or not the media should be recorded in encrypted form or in decrypted form. If recording can be done in decrypted form, theoretically every solution can record the media, since they can all provide the keys to the network servers one way or another.
However, if the media should be recorded in encrypted form, only the solutions in which the keys can be exchanged without dependency of the availability of the endpoints can satisfy this requirement. This implies that SDES, IMSKAAP, DTLS-SRTP and Zfone are not able to support this requirement without additional extensions, because these protocols need some way of storing the key with the recorded media, in order to provide it to the user endpoint when becomes available again. TBS and Otway-Rees do satisfy this requirement completely, since their use of a KMS provides the possibility to exchange keying material when one of the user endpoints is offline and comes online later on.

3gpp.25: *Multiple solutions should be avoided to reduce complexity in the network and to maximise interoperability between user devices*
Since SDES, IMSKAAP, DTLS-SRTP and Zfone are solutions specifically designed for SRTP and not able to meet all the extra 3GPP requirements by itself adjustments or a combination of solutions are needed to fulfil all requirements, and therefore they fail this requirement.
TBS and Otway-Rees are specifically designed for IMS, but are not able to meet all the requirements by itself as well. Since the specific design for IMS, the failed requirements may have to be reconsidered in order to check whether the use of multiple solutions should be preferred above the failed requirements. This may imply that TBS and Otway-Rees are not the perfect solutions for IMS, but the most suitable instead and then they meet this requirement.

3gpp.26: *The requirement for new functions on the user's smartcard should be avoided unless it would provide significant and cost effective benefits*

Every solution meets this requirement.

3gpp.27: *The solution should support the possibility to protect user traffic on an end-to-end basis between IMS-capable and non IMS-capable user equipment*

TBS, Otway-Rees and IMSKAAP are IMS specific solutions and non IMS-capable user equipment will most probably not support these methods.

SDES is the current de facto standard key management mechanism for SRTP and DTLS-SRTP is assumed to be the future standard and therefore these solutions are relevant to non IMS-capable devices.

Zfone can be used by any device which is able to run Zfone and to set up an RTP connection.

3gpp.28: *The solution shall have minimal impacts on already deployed network entities*

TBS and Otway-Rees need a Key Management Server (KMS), which has to be deployed in existing nodes or in new nodes. Communication between the KMS and other nodes must be secured by security associations in order to fulfil security requirements within the core network.

IMSKAAP needs adjustments of the S-CSCF servers in order to compute the keys, however these adjustments are almost minimal (see paragraph 4.2.4). SDES, DTLS-SRTP and Zfone do not need adjustments in the network nodes.

However, for each solution applies that when termination of security should be done in network elements, then all of these elements will be influenced.

3gpp.29: *A media security solution shall assume that messages cannot be sent over the media path until the media session has been established*

Every solution meets this requirement.

3gpp.30: *A media security solution shall assume that only media traffic can be sent over the media path*

Both DTLS-SRTP and Zfone fail this requirement, since both solutions use the media path for negotiating the security associations.

3gpp.31: *Media security solutions for media protection and key management shall cover both end-to-end and end-to-middle media protection scenarios*

Every solution meets this requirement.

4.1.5 Scalability, Cost and Performance

Scalability, Cost and Performance						
ID	TBS	SDES	Otway-Rees	IMSKAAP	DTLS-SRTP	Zfone
3gpp.34	OK	OK	OK	NOK	OK	OK
3gpp.35	NOK	OK	NOK	OK	OK	OK
3gpp.36	OK	OK	OK	OK	OK	OK

Table 4.5 Analysis of the Scalability, Cost and Performance requirements

3gpp.34: *The solution should scale well for large users*

TBS and Otway-Rees make use of an KMS, which is very suitable for scaling, while SDES, DTLS-SRTP and Zfone do not make any effort in the network. IMSKAAP, however, is the only solution in which the S-CSCF servers have to do computative operations. This will impede scaling because there has to be much more computing power when there are many users.

3gpp.35: *The solution should be cost effective*

The TBS and Otway-Rees methods both need a KMS infrastructure which has to be deployed, but the costs of the infrastructure are yet to be determined. Also the complexity in terminal support is still unknown since the protocols have to be developed. Therefore these methods cannot meet this requirement yet.

3gpp.36: *The solution should not adversely affect performance of IMS services. In particular, there should be no significant increase in call set-up delay and no media clipping*

The IMSKAAP method is the method of which I suppose it will affect IMS services performance most. Both the clients as the servers all have to do Diffie-Hellman computations and all have to communicate the necessary data. All other methods depend only on extra signalling and therefore I assume IMSKAAP to be the most performance affective. However, IMSKAAP is the only method which has been tested in a simulation run [12] and conclusions were that it has a minimal delay compared to session with no end-to-end security and much less delay compared to (outdated) security mechanisms as IPsec and TLS. Therefore it may be seen as an efficient suitable mechanism for media plane security.

The extra signalling to the KMS may affect the performance of the IMS services, but the communication between KMS and user equipment is minimal and assumed to be less performance affective than Diffie-Hellman computations. Therefore these methods will probably meet the requirement.

DTLS-SRTP and SDES meet the requirement, since there is respectively minimal and no overhead in session setup.

According to the Zfone developers Zfone does increase the call setup delay with approximately two seconds. However, this delay can be overcome and during the call the end-user won't notice any delay, so Zfone meets this requirement as well.

4.1.6 Access network

Requirements regarding the access network type						
ID	TBS	SDES	Otway-Rees	IMSKAAP	DTLS-SRTP	Zfone
3gpp.37	OK	OK	OK	OK	OK	OK
3gpp.38	NOK	OK	NOK	OK	OK	OK
3gpp.39	OK	OK	OK	NOK	OK	OK

Table 4.6 Analysis of the requirements regarding the access network type

3gpp.37: *The solution shall support the possibility to provide protection on an end-to-end basis between any IMS-capable user endpoint regardless of what type of access technology they use*

Every solution is access independent and therefore they all meet this requirement.

3gpp.38: *The key management solution should be based on the existing IMS access security architecture, so that no special user registration or user involvement is required and so that existing infrastructure can be re-used*

For TBS and Otway-Rees the infrastructure must be enhanced, because a KMS has to be deployed, but all other methods reuse existing infrastructure and do not require user involvement.

3gpp:39: *Since the IMS client may use different access authentication methods, the key management solution for end-to-end security shall be able to work independently of any of these authentication methods*

IMSKAAP needs cipher material established during the UMTS AKA registration procedure of the mobile device to the IMS servers. It uses this material in fundamental steps of the

procedure and unless IMSKAAP creates a new method for creating similar cipher material it depends heavily on the IMS access authentication method.

4.1.7 Backward compatibility and migration

Backward compatibility and Migration						
ID	TBS	SDES	Otway-Rees	IMSKAAP	DTLS-SRTP	Zfone
3gpp.40	N/A	N/A	N/A	N/A	N/A	N/A
3gpp.41	OK	OK	OK	OK	OK	OK
3gpp.42	OK	OK	OK	OK	OK	OK

Table 4.7 Analysis of the backward compatibility and migration requirements

3gpp.40: *Media security shall be mandatory to implement for user endpoints and networks and optional to use for user endpoints*

This requirement is not applicable to the solutions.

3gpp.41: *The media security solution shall allow a user endpoint to negotiate media security settings for each individual call*

All the solutions allow the user endpoint to negotiate media security settings for each individual call.

3gpp.42: *The negotiation of media security must be protected against downgrading attacks*

All the solutions depend on the SIP security with respect to the downgrading attack. Downgrading could still be possible by replacing the SRTP media description in the SDP message by one which only contains RTP. When making the security visible to the user downgrading attacks can be mitigated for sure.

4.1.8 Other requirements

Other requirements						
ID	TBS	SDES	Otway-Rees	IMSKAAP	DTLS-SRTP	Zfone
3gpp.44	OK	OK	OK	OK	OK	OK
3gpp.45	OK	NOK	OK	NOK	NOK	NOK
3gpp.46	OK	NOK	OK	NOK	NOK	NOK

Table 4.8 Analysis of the other requirements

3gpp.44: *A solution shall support the possibility to protect RTP-based IMS user plane traffic*
This is the main objective of the 3GPP within the topic of IMS media security, therefore all solutions fulfil this requirement.

3gpp.45: *A solution shall support the possibility to protect non RTP-based IMS user plane traffic. If a single solution leads to undue complexity or delay in standardisation or deployment it may be acceptable to standardise more than one solution. If multiple solutions are standardised, then they shall be defined within a single framework*
SDES, IMSKAAP, DTLS-SRTP and Zfone are only defined for setting up security associations for SRTP. However, with small adjustments to the specifications these solutions can also be used for setting up security associations for non RTP-based traffic.
TBS and Otway-Rees could be used for other purposes than securing SRTP only. However, since these solutions are not fully developed yet, exact use is still for further study.

3gpp.46: *A solution shall support the possibility to protect application layer messages, e.g. SIP MESSAGE*
SDES assumes secure signalling through which SDES is secured and which implies that the SIP message is secured as well. However, SDES is not able to secure a SIP message itself.
IMSKAAP is only defined for use with SRTP. It also does not rely on secure signalling, but it uses SIP messages as carrier of the protocols data and therefore this protocol cannot be used to secure these messages.
DTLS-SRTP and Zfone are only defined for use with SRTP. Adjustments are needed to use these solutions for other purposes than SRTP. However, these solutions use ports which are defined in the SIP messages and therefore they cannot be used in advantage to setup secure signalling.
TBS and Otway-Rees could be used for other purposes than securing SRTP only. However, exact use is still for further study.

3gpp.47 – 3gpp.52: These requirements are not applicable since they do not affect the security solutions directly, but are more user interface related, or they have already been addressed by previous requirements.

4.2 Architectural analysis

The core architecture of the Open Source IMS Core system has been presented in Figure 1.5 and all proposed solutions will impact this architecture to a certain extent. This chapter will illustrate this impact and discuss the implications of the architectural changes for the application of those solutions.

4.2.1 Ticket-Based System

To develop the Ticket-Based System in the Open Source IMS Core environment new functions have to be deployed within the overall architecture. Figure 4.1 shows how the Open Source IMS Core architecture has to be extended in order to deploy the TBS. The added functions are an independent Key Management Server and the Bootstrapping Server, which is used for setting up a secure connection between User Endpoints and the KMS.

The Bootstrapping functionality might be taken over by the Generic Bootstrapping Architecture (GBA) of the IMS platform, which implies that it would not have to be developed from scratch. The Open IMS Playground offers such a GBA system and could be hooked up to the Open Source IMS Core quite easily.

The development of the KMS can be done by implementing it as an Application Server, letting it function as an extension to the IMS platform. This offers the possibility to have the KMS operated by a third party. Since fetching the key only depends on possession of the ticket (see Figure 2.5), lawful interception by the IMS operator is still enabled, while the KMS is be deployed by a third party. This may be cost effective for IMS operators and opens up market opportunities for other companies. The negative side effects are that this third party must be trusted and offer the same security as the IMS platform, since there will be another point of failure in the security chain.

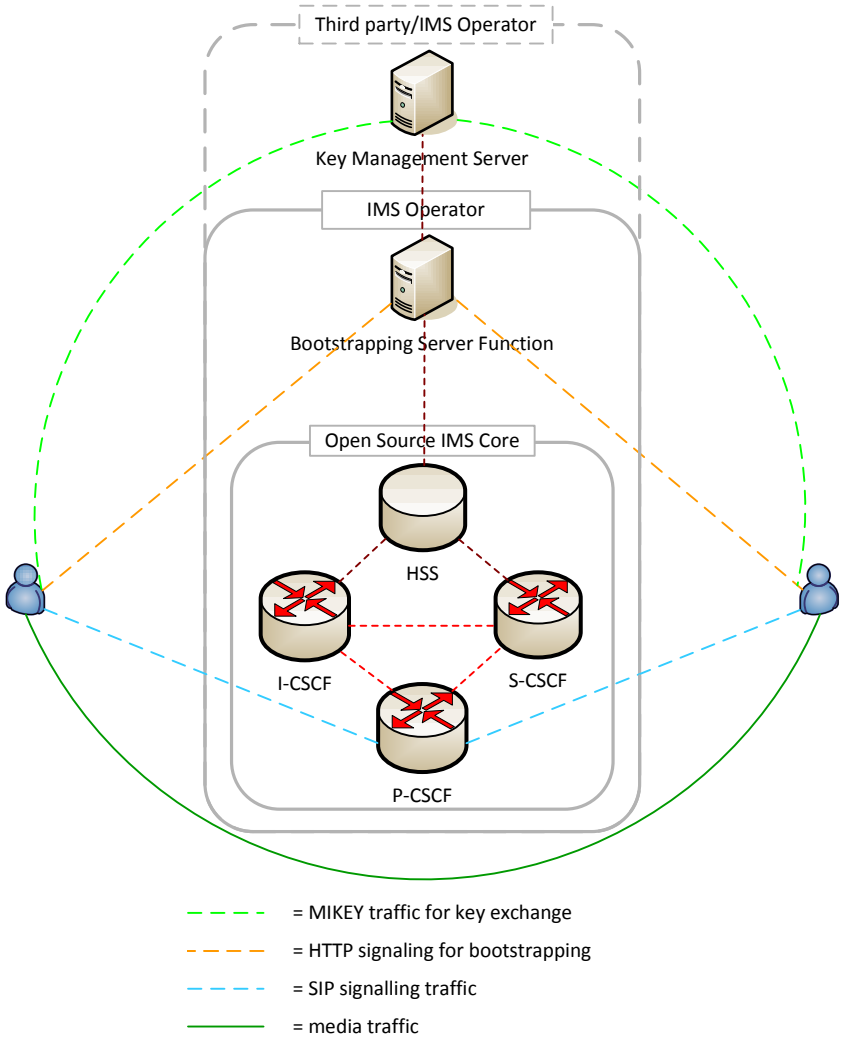

Figure 4.1 Ticket-Based System architecture

4.2.2 Otway-Rees

Figure 4.2 illustrates the architecture of the Otway-Rees solution and it looks very similar to the TBS solution. In fact, both are very similar protocols and offer similar functionality.

The main architectural difference between both solutions is that the Key Management Server of the Otway-Rees solution cannot be managed by a third party. The reason for this is that for lawful interception the KMS has to be managed by the IMS operator, since there is no possibility for the CSCF-functions (or a specific LI function) to intercept messages and fetch the key by means of a ticket. Instead, only the KMS knows the keys and may send them to the correct users, based on specific policies. Therefore, if the IMS operator controls the KMS, it can control the policies, enabling lawful interception by granting operator-functions access to the keys.

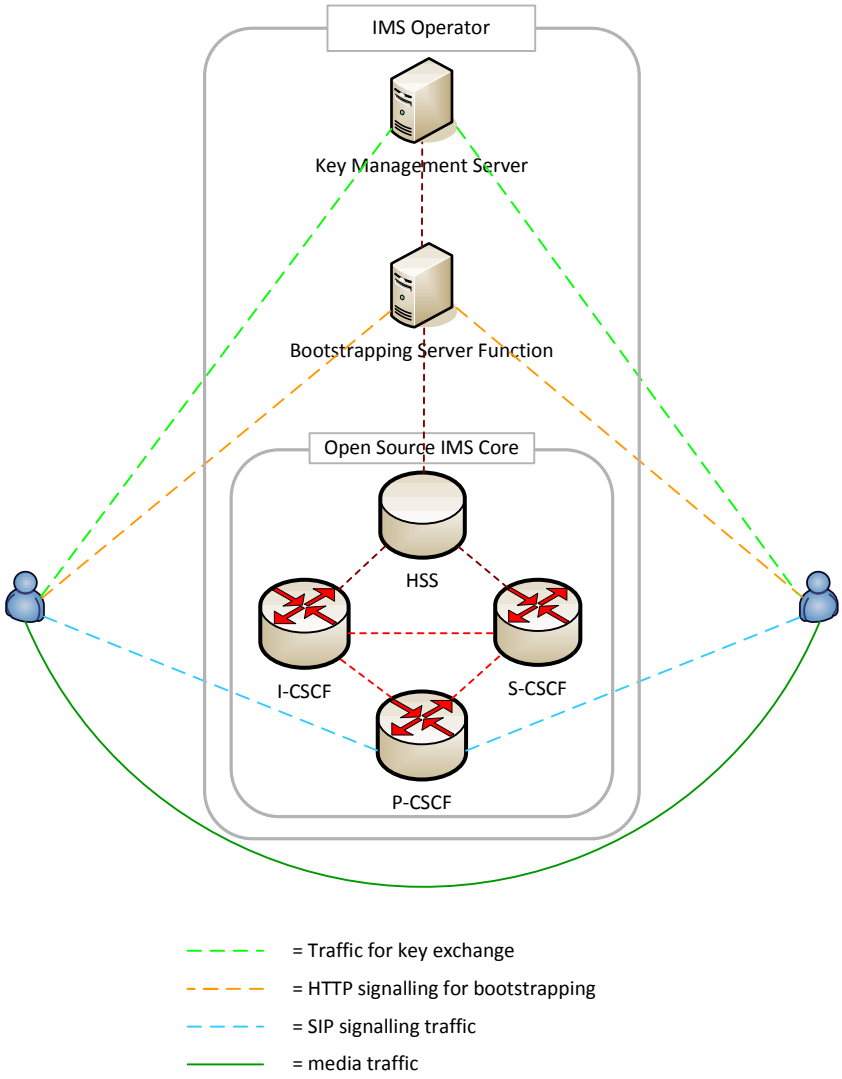

Figure 4.2 Otway-Rees architecture

Such an architecture implies that the IMS operator should develop and run the KMS and a lawful interception function (which may be present in a CSCF), and that this function will be a core function in the operators architecture. This has the consequence of less points of failure in the security chain, but increasing cost and responsibility for the IMS operator.

4.2.3 SDES

The impact of SDES on the serverside architecture is nihil. Figure 4.3 illustrates that no extra functions have to be added and that setting up a secured media connection can be done without intervention of the IMS servers. Even with this architecture lawful interception is

enabled by scanning the SIP messages for the 'a=crypto' attribute in the P-CSCF or S-SCSF nodes.

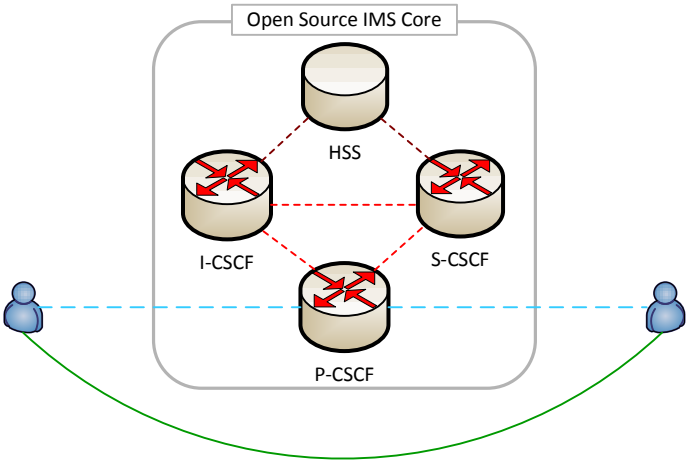

Figure 4.3 SDES architecture

4.2.4 IMSKAAP

The architecture of IMSKAAP is very similar to the SDES architecture, see Figure 4.4, but the difference is that adjustments must be made to the S-CSCF node. The S-CSCF is a core node in the IMSKAAP procedure for computing keying material (see Figure 2.7) and this computing functionality has to be added to the server node. Since all communication is done through SDP extensions in the SIP message no alternative communication channel has to be setup. Since the S-CSCF computes the keys, lawful interception is enabled.

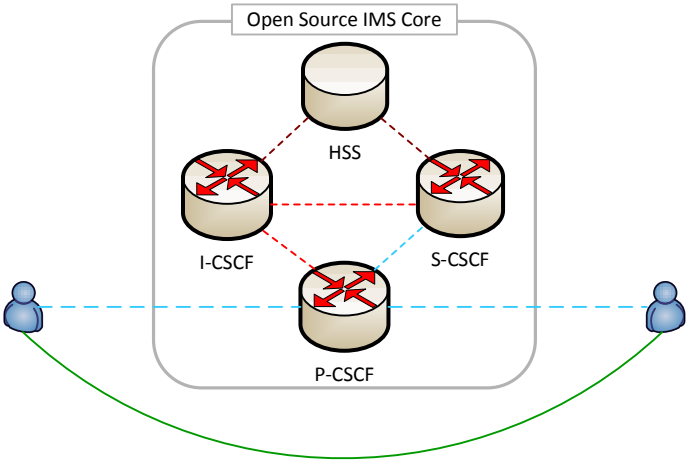

Figure 4.4 IMSKAAP architecture

4.2.5 DTLS-SRTP

When lawful interception isn't an issue, the DTLS-SRTP solution is a solution which doesn't impact the IMS architecture at all, see Figure 4.5. The keying material is negotiated outside the IMS architecture over its own communication channel, with only the DTLS fingerprint sent within the SIP messages over the IMS architecture. This fact makes lawful interception very hard, since the IMS nodes don't have the ability to retrieve the keys.

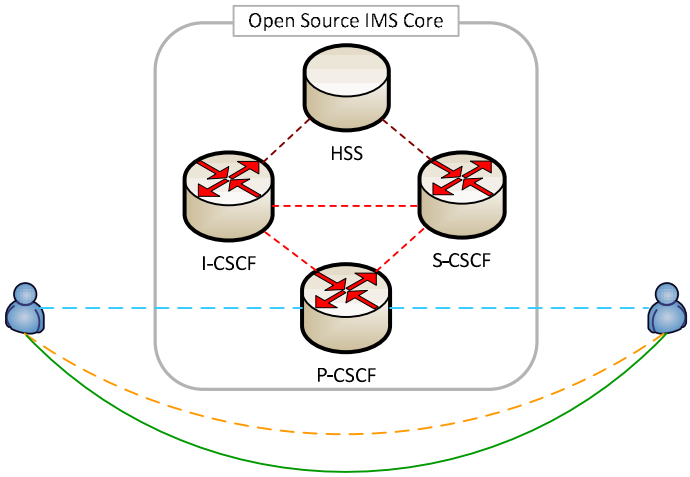

Figure 4.5 DTLS-SRTP architecture

The proposed solutions to enable lawful interception, like demanding the user to send the key to the IMS nodes in order to establish a connection can be achieved with the architecture in Figure 4.5, however these solutions are easy to mislead or very hard to realize.

4.2.6 Zfone

This solution has a very similar architecture to the DTLS-SRTP solution except for the fact that the key exchange is done over the media path, thus using exactly the same communication channel instead of setting up keying material over its own channel. Figure 4.6 illustrates this architecture. It also makes clear that lawful interception is not feasible when this kind of key exchange solution is used.

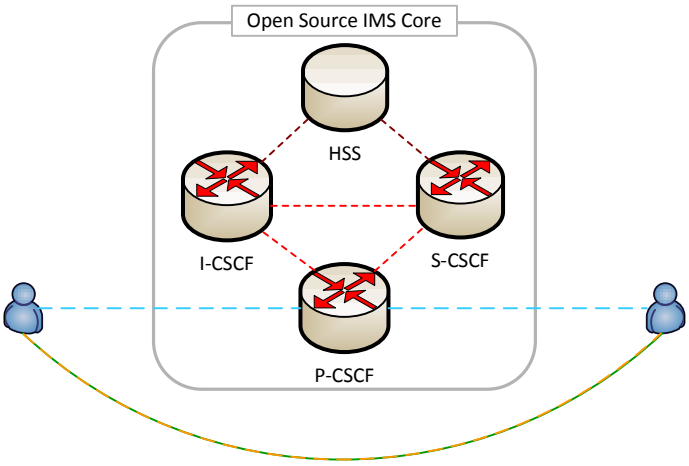

Figure 4.6 Zfone architecture

4.3 Proof of Concept

This section describes the implementation of the Proof of Concept and practical problems encountered during the implementation phase. It discusses the practical Open Source IMS Core environment and architectural issues one has to work with during implementation and it tries to identify the issues regarding the practical software engineering situation as stated in paragraph 1.6.

4.3.1 Overall architecture

Since Open Source IMS Core is an open source system without a well documented software architecture we have to find out the architecture ourselves. Figure 4.7 gives an simplified overview of how the system is composed and it shows the most important files where adjustments are needed. This overview is created using the directory structure of the open source system.

Figure 4.7 illustrates that the Open Source IMS Core is build out of two main parts: the HSS server, called FHoSS and the Ser_IMS. The HSS server is an independent application to which no adjustments are needed. It can be started by calling the startup script. The Ser_IMS is the core of the SIP Express Router (SER) and is used as the foundation for all the CSCF servers. Every single CSCF server is an module extending the Ser_IMS and they all run as independent instances. These modules handle the core functionality of the servers, like routing messages and offering interfaces. Besides these CSCF modules, the system consists out of many more modules offering the functionality outside the CSCF core functions but needed for operation of

the whole system, however for simplicity reasons these modules are not part of the illustration. Next to the modules packages there are some packages just for development purposes, which I have called Config 1 to Config n and a Parser package for parsing all the incoming and outgoing messages.

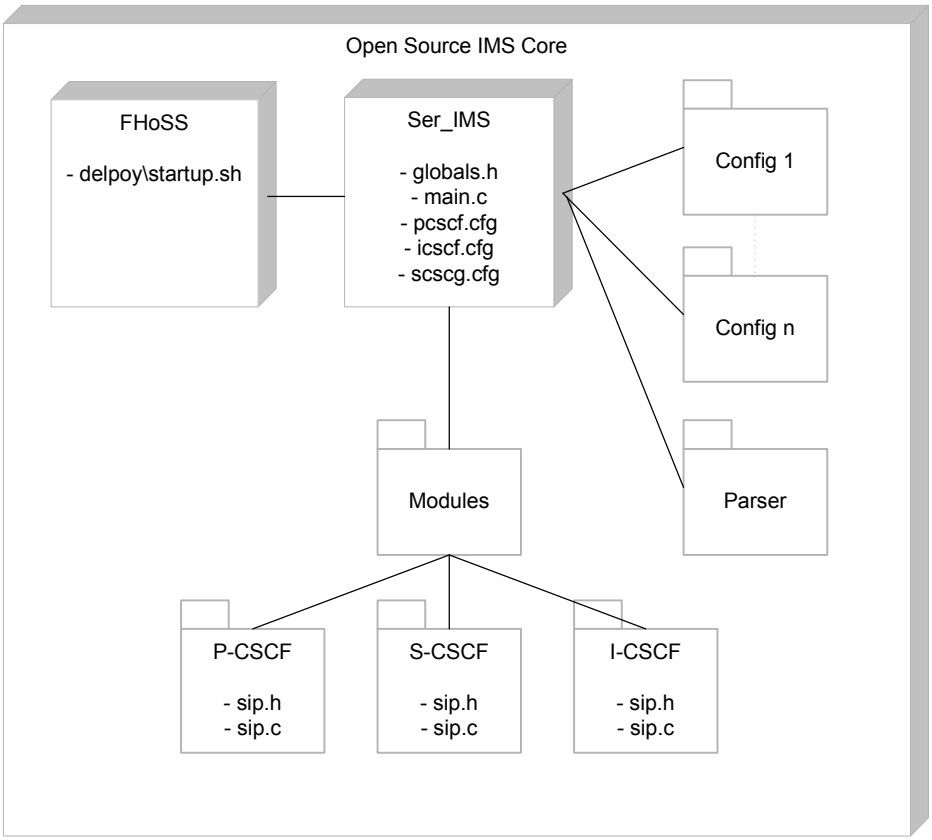

Figure 4.7 Open Source IMS Core directory structure

Open Source IMS Core is based on SIP Express Router (SER) and is mainly implemented in C. Since every CSCF server can be configured using the right configuration file, which are written in a semi C-language. These configuration files are interpreted by the main application and they handle setup of the servers by loading the right modules and routing of the SIP messages by special written routing logic.

The globals.h file contains all the global variables and parameters and defines which data structures are used and main.c file is the main startup file.

As already mentioned modules are used to extend the functionality of one of the servers. In fact the CSCF servers are modules themselves, extending the SER. So extending a server is relatively easy, since the functionality can be put in several functions distributed over well-chosen files. These files combined together will form the module and a calling function/statement at the right place in the already existing server files will enable the added module.

4.3.2 Implementation

By means of illustration I have implemented a Proof of Concept of the SDES solution, since this solution does not need massive adjustments and additions to the Open Source IMS Core architecture which time constraints prohibited. The implementation shows how relatively easy it is to implement media security in Open Source IMS Core, considering the lawful interception requirements and it shows the relative ease within a practical environment, if the problems encountered in the previous section have been overcome.

Besides adding functionality to the Open Source IMS Core, the UCT IMS client should be altered as well, in order to setup an SRTP connection using SDES. However, altering the client goes beyond the topic of this thesis and therefore will not be discussed here.

The functionality which has to be added to the server is the attribute detection in the SDP attachment of the SIP messages. Since key negotiation will be handled during setup of the conversation the INVITE messages have to be checked for such an attribute. Therefore a rule has to be added to the main routing logic of the S-CSCF which calls a function if the message is an INVITE. The following code realizes this:

```
if(method=="INVITE") {
      # call method which checks for a=crypto in SDP
      cscf_check_sip();
}
```

The question where to locate the `cscf_check_sip()` method can be answered by checking the core functionalities of the different CSCF servers. Since the I-CSCF handles only routing issues, the P-CSCF is only the contact point for the UE with the IMS platform and S-CSCF is the central node of IMS handling registration processes, making routing decisions, maintaining session states and storing service profiles the S-CSCF seems to be the proper node

for checking the SIP message for the SDES attribute. However, since both P-CSCF and S-CSCF are on the path of every SIP message, they are both able to inspect all the messages. Therefore, one could argue for adding the checking functionality to the P-CSCF. I will use the S-CSCF, since this server is used for all SIP processing and the other server are used for routing.

The following fragments implements the checking functionality and prints the message to a log file if it finds an SDES attribute. This method is located in the sip.c file, since this file handles all SIP message functionality.

```
/**
*           check for a=crypto attribute and print
*           the message to a log file
*           @param msg – the message to print
*           @return 1 on succes or 0 on error
*/
int cscf_check_sip(struct sip_msg* msg) {
      char* crypto = "a=crypto";
      char* sdpbody = msg->unparsed;
      str sipstr = msg->first_line.line;
      char* sip = sipstr.s;

      if (find_string(sdpbody, crypto)) {
            LOG(L_INFO,"INF: Printing the SIP message \n");
            LOG(L_INFO, "INF: sdpbody is: %s\n",sdpbody);
        if(write_sip_to_file(sip)) {
            LOG(L_INFO, "INF: Writing SIP to file established!!\n");
                  return 1;
            } else {
                  LOG(L_ERR,"ERR: writing sip to file failed!!!\n");
                  return 0;
            }
      }
      else {
            LOG(L_ERR, "ERR: No a=crypto found! \n");
            return 0;
      }
}
```

The method filters the SDP body of the received message '`msg`' and calls the method `find_string()` to search in the SDP body for the crypto attribute. If the attribute is found it gives feedback to the LOG output and it writes the whole SIP message to a log file using `write_sip_to_file()`. It may be clear that instead of writing the whole SIP message to a file one may add other functionality for retrieving the key out of the body of the attribute and use this key for intercepting and decrypt an existing SRTP stream. This functionality has not

been added in this project, due to time constraints and the fact that no client was able to setup an SRTP connection using SDES over the Open Source IMS Core environment.

The following fragment is used for writing the SIP message to a log file.

```
/**
*           print the sip message to a log file
*           @param sip - the sip message to print
*           @return 1 on succes or 0 on error
*/
int write_sip_to_file(char* sip) {
      FILE *f;

      f=fopen("home/gelderasv/scscflog/log.txt","a+");
      if (!f)
        return 0;
      fprintf(f,"%s\n",sip);
      fclose(f);
      return 1;
}
```

5 Conclusions and Discussion

This chapter discusses the results from the previous chapters and the conclusions drawn from it. The discussion will be held per solution and the method for drawing conclusions will be based upon elimination of solutions: the discussion of the results of previous chapter will make clear that several solutions are definitely not suitable for use within an IMS system, and therefore these solutions will be eliminated as a possible solution.
Moreover the Proof of Concept will be discussed and the answers to the research questions from section 1.6, which have been presented along the whole thesis, will be extracted and recapitulated.

5.1 Zfone-like applications

As Table 4.1 illustrates Zfone-like applications are not capable of setting up a secure connection which is able to be lawfully intercepted. Since the 3GPP is designing the IMS platform for commercial purposes and eventual use by telecom operators, this requirement is very strict. Lawful governments demand by law from telecom operators that there must be a possibility for eavesdropping secure communication channels by the government, if the operators offer such secure communication channels as a commercial service [11]. Therefore failing this requirements already leads to the conclusion that Zfone or Zfone-like applications are not suitable for commercial use in an IMS platform, even more since there are no suitable workarounds to solve this failed requirement.

Other reasons for eliminating this solution are that Zfone does not meet the 3ggp.6 and 3gpp.24 requirements, since it does not offer a satisfactory level of security and satisfy interception requirements simultaneously and secure voicemail is a problem since there is no way to store the key for decrypting the recorded encrypted media.

Furthermore Zfone cannot be used for secure multiparty communication, whereas secure multiparty communication may be an important requirement in the corporate market, since conference calls may be a large part of all corporate communication. And since IMS is a platform enabling IP-based access independent multimedia services, corporate multiparty conferences must be considered as a potentially large user group.

Another drawback of Zfone is that it is a solution specifically developed for (end-to-end) SRTP and although it might be extended without large effort, it is a very concrete solution to a specific problem. Therefore Zfone is, compared to TBS or Otway-Rees, much less practical to use within an environment which demands extension and adaption and may be marked as less 'future-proof' than TBS and Otway-Rees.

The final drawback concerning Zfone regards the adjustments which have to be made to network nodes. Zfone has to use the media path for negotiating its security associations and therefore other non-media data has to be transported over that path. However, since IMS nodes are designed for and only capable of transporting media traffic, some nodes have to be adjusted in order to enable the Zfone protocol. Therefore, other solutions are more suitable than Zfone.

The cost effectiveness and well scaling advantages make no odds against the previous mentioned drawbacks, with the failed lawful interception requirement in particular. Therefore the conclusion is that Zfone or Zfone-like applications are not suitable for commercial use in an IMS platform.

Conclusion 1:	Zfone or Zfone-like applications are not suitable for commercial use in an IMS platform

5.2 DTLS-SRTP

As Table 4.1 points out for DTLS-SRTP as well, lawful interception is not possible with the use of DTLS-SRTP as a solution for media security. Since this is a very strict requirement for commercial platforms, DTLS-SRTP is already eliminated by this requirement. Furthermore it also suffers from the same other drawbacks as Zfone and therefore the same conclusion can be drawn, although DTLS-SRTP, unlike Zfone, is able to setup secure multiparty communication.

Conclusion 2:	DTLS-SRTP is not suitable for commercial use in an IMS platform

5.3 IMSKAAP

IMSKAAP is an elegant solution, with architectural and security benefits, but it has a few important drawbacks. The first drawback is that IMSKAAP is not able to setup secure multiparty communication, while as already mentioned in section 5.1, secure multiparty communication should be considered as a potentially important requirement, since corporate users might use this feature often. Next it fails the recording of encrypted media requirement as well, neglecting the probably desirable need by many customers for a voicemail.

Furthermore IMSKAAP demands from the S-CSCF servers to compute Diffie-Hellman values for each single user and when the solution is scaled up to a scale for commercial use I expect the S-CSCF servers to be impacted heavily and have a large degraded performance. Since the S-CSCF servers are core nodes of the IMS platform, degraded S-CSCF performance will directly impact the performance of the whole IMS system and in a commercial context this is not acceptable. Therefore the conclusion will be that IMSKAAP is not suitable for commercial use in an IMS platform.

Next to Zfone and DTLS-SRTP, IMSKAAP is a solution specifically designed for SRTP as well and therefore it is less 'future-proof' than TBS or Otway-Rees.

Although IMSKAAP benefits from the same advantages as Zfone and DTLS-SRTP, the previous mentioned drawbacks are too important and therefore this solution is eliminated as a possible solution.

Conclusion 3: IMSKAAP is not suitable for commercial use in an IMS platform

5.4 SDES

SDES is a solution which has many advantages and only a few (minor) disadvantages. Almost all requirements are met of which the most important and most attractive will be discussed here: The solution has very minimal architectural impact and is very easy to implement, as well in the client as in the server, of which the last is shown by the Proof of Concept. Furthermore does it meet all the security requirements, is it well scalable and very cost effective and is it an already IETF standardized and fully developed protocol, which all together makes it a highly desirable solution for implementation.

A minor drawback of SDES regards secure multiparty communication without the server knowing the key. In this case one should estimate the risk of having the server knowing the group key, since the server is part of the IMS network and therefore protected by the network security. This should provide a security level which is high enough for normal customer use and in fact for most corporates as well, since the traditional telephone situation offers similar security. Therefore this failed requirement is not a major drawback and does not eliminate SDES as a candidate solution.

Another problem is, just like the previous solutions, the specific design purpose of SDES. It is specifically designed for use with SIP and SDP and to setup SRTP connections. The purpose of only setting up an SRTP connection makes it less flexible and less 'future-proof' than the TBS and Otway-Rees protocols, and the use of SIP and SDP creates even another drawback, since the security of SDES depends on the security of SIP and SDP. However, the SIP and SDP security may be assumed to be secure and as already mentioned SDES does meet the security requirements, so therefore this argument is of less importance.

Until now I think the big advantages of low cost, minimal architectural impact and ease of implementation may outweigh the mentioned disadvantages. However, SDES has one major drawback and it concerns the recording of encrypted media. It is not able to fulfil the requirement about recording of encrypted media whatsoever, and there is also no extension for SDES enabling the solution to offer encrypted media recording. Although all previous mentioned solutions did not offer this as well, they also lacked other very important requirements which SDES does not, thus making SDES a possible interesting solution. Therefore it might be interesting to look for workarounds, for example by the use of multiple solutions, in order to offer the possibility for encrypted media recording. However, these are thoughts for future research, in which a balanced decision should be made and on which this thesis cannot give an answer. Therefore, for now this lack of media recording and thus of secured voice mail leads to conclusion 4.

Conclusion 4: SDES is not suitable for commercial use in an IMS platform when encrypted media recording is required

5.5 Otway-Rees/Ticket-Based System

The Otway-Rees and the Ticket-Based System (TBS) will be discussed together in this section, because the results from the previous chapters made clear that Otway-Rees and TBS operate as similar systems, have similar properties and have more or less the same outcome of both the requirement analysis as the architectural analysis. The systems have minor differences in the protocol for message exchange, which only results in a different way of implementing the lawful interception functionality.

TBS and Otway-Rees are very suitable solutions for a commercial IMS context, since they meet almost every requirement except the ones discussing adjustments to the current system and costs and implications on development.

The expected high costs are a consequence of the new infrastructure which has to be deployed and it may be clear that these costs will be much higher than those of the other solutions. However, due to the premature phase of development of these solutions, an exact estimation of the costs cannot be made. Costs, however, should not be the main obstacle in developing or choosing one of the solutions; in general, investments should be made in order to gain in the long term and therefore further research should be done to the costs and benefits of these solutions.

The architectural requirements failed by these solutions deal with the possibility to protect user traffic between IMS-capable and non IMS-capable user devices (3gpp.27), the minimal impact on the existing architecture (3gpp.28) and with the idea that the key management solution should be based on the existing IMS access security architecture (3gpp.38).

In comparison to, for example, SDES failing 3gpp.27 is a minor drawback, but one may question the responsibility of the IMS operator for secure connections setup outside the platform. Furthermore the capabilities of TBS and Otway-Rees at the other requirements and the possibility for flexible extension for future products make failing 3gpp.27 a very minor issue.

The impact of both the solutions on the architecture (3gpp.28) however, is quite large, which has the consequences of enabling more points of failure, a more difficult implementation and

probably (much) higher costs in the final development. Therefore this makes TBS and Otway-Rees much more unattractive as a final solution, and one has to balance the very attractive side of these solutions against this very minor one. But as already mentioned, costs should not be an issue at this point development.

Also 3gpp.38 is marked as failed, because TBS and Otway-Rees need an extra registering phase with the Bootstrapping Server Function and furthermore it demands the infrastructure to be enhanced, in order to provide the Key Management Server's and the Bootstrapping Server's functionality. However, the extra registering phase can be taken care of by the Generic Bootstrapping Architecture (GBA), which is an already existing functionality, handling security and authentication between user devices and Application Servers. Since IMS offers the possibility to incorporate GBA, this requirement may be marked as passed. However, with respect to the research question of this thesis, both TBS as Otway-Rees are unattractive solutions.

Conclusion 5: TBS and Otway-Rees are considerably most cost and architectural extensive and therefore they are not attractive for development; however exact costs cannot be determined yet

As mentioned, both solutions meet all the other requirements. Furthermore their architecture enables a framework for negotiating general security parameters, and thus offering easy possibility for extensions and adaptation. These properties make them very suitable for use within a commercial IMS context and therefore the discussed drawbacks should be weighed accurately in order to come to a mature media security system.

Conclusion 6: TBS and Otway-Rees are most 'future proof' and therefore commercially most interesting

5.6 Proof of Concept

The implementation of the Proof of Concept gives a clarifying overview of the practical architecture of Open Source IMS Core, which consists out of well-organised modules, and made clear that SDES is a very simple and attractive solution from implementation point of view. However, the relative ease of this implementation might also make one think about the

hardness of implementing the TBS or Otway-Rees solution: of course, they needs a much more thought-through detailed architecture, a well-planned schedule and a solid financial plan, but Open Source IMS Core is based on modules and therefore extending the core functionality is relatively easy, also for larger systems. This offers the best situation possible for implementing a KMS solution such as Otway-Rees or the Ticket-Based System.

5.7 Summary and recommendations

As concluded before IMSKAAP, DTLS-SRTP and Zfone are not suitable for use in an IMS environment. They lack the lawful interception requirement, which is a must in commercial contexts.

SDES is a solution which meets many requirements, but is not able to record encrypted media and is less 'future proof' then TBS or Otway-Rees due to its limited SRTP purpose. However, costs and architectural impact are very minimal, which is also proved by the Proof-of-Concept. This makes it a very attractive protocol.
The drawback of SDES is its dependability of secure SIP signaling. This makes it as stand-alone solution very vulnerable. However, the IMS security may be considered sufficient in order to make SDES a successful solution.

TBS and Otway-Rees are both very similar protocols offering the same functionality, differing only in the protocol for message exchange. These two solutions offer, among other things, the possibility for encrypted media recording and multiparty communications, which the other solutions lack. Furthermore do they offer lawful interception and the possibility to be used for other purposes than SRTP only.

The drawbacks of these protocols are the fairly large adjustments to the architecture and the expected high costs that go with it, making it less suitable for development and financially less attractive.

In order to make a final decision between a KMS solution, like TBS and Otway-Rees, and SDES, further research has to be done to the costs of the TBS or Otway-Rees development, the opportunities for usage of these systems and the willingness of companies to develop such a

large system. After all, implementing SDES is much easier and cheaper, but it offers fewer opportunities for extension and appliance for future products.

5.8 Research questions

This section recapitulates the research questions formulated in section 1.6 and gives concise answers to them.

- Inventory of solutions
  - Which protocols may be used for media security?

    DTLS and SRTP might be used as en encryption protocol, however the 3GPP has stated to use SRTP within its IMS systems.
  - Which key exchange protocols may be used?

    SDES, DTLS-SRTP, IMSKAAP, Zfone-like applications and protocols, Ticket-Based System and Otway-Rees are the solutions which may be used for key exchange within IMS.
  - What are the currently proposed solutions by other parties?

    IMSKAAP is a solution proposed by the Taiwanese researchers Chen et al.

    Zfone-like applications are solutions based on the ZRTP protocol, developed by Phil Zimmermann for use with Voice-over-IP.
- Requirements analysis
  - What are the requirements for key exchange for IMS?

    see section 2.2.2.
  - Which requirements do the proposed solutions meet?

    see section 4.1.
  - Which solution matches the requirements best?

    There is no solution meeting all the requirements, but TBS and Otway-Rees meet the most and the most important ones.
- Architectural consequences
  - What is the impact of the solutions to the Open Source IMS Core architecture?

    see section 4.2
  - Which solution is the best solution from architectural point of view?

    SDES is the most easy solution to implement, considering the 'must-have' lawful interception requirement.

- Selecting a solution
  - Considering the requirements analysis and the architectural consequences, which solution has the overall best results?

    TBS, Otway-Rees and SDES have a similar outcome and depending on ones considerations a choice should be made; see section 5.
  - Which open source solutions are already available?

    No open source solution was available.
  - What are the practical boundaries and problems for implementing a solution?

    No architecture is available for Open Source IMS Core and therefore a detailed research to how the system works has to be done.

    No SRTP clients have been available, so testing whether the server is able to decode SRTP streams was not possible.

The main research question of this thesis: ***'Which solution for offering media security is most suitable for Open Source IMS Core considering the security requirements stated by 3GPP and considering the practical software engineering situation?'*** has not a direct answer. If one would consider the strict time-limits of writing this thesis as the practical software engineering situation, one could say SDES is the solution most suitable for Open Source IMS Core. Also if one would see the architectural impact and the expected high costs as the practical software engineering situation SDES should be the answer. However, I think a KMS solution like TBS or Otway-Rees is the solution which is most suitable for commercial IMS, since it is the most flexible system and offers the most possibilities for future products. Therefore, in order to make a final decision between TBS or Otway-Rees and SDES, further research has to be done and a decision should be made later on.

6 References

1. Poikselkä, M., Mayer, G., Khartabil, H., & Niemi, A. (2006). *The IMS: IP Multimedia Concepts and Services*. (Second edition). Chichester: John Wiley & Sons, Ltd.
2. wikipedia.org. (2008, 29 October). *IP Multimedia Subsystem*. Wikipedia [online encyclopedia]. http://en.wikipedia.org/wiki/IP_Multimedia_Subsystem
3. Chakraborty, S., Frankkila, T., Peisa, J., & Synnergren, P. (2007). *IMS Multimedia Telephony over Cellular Systems*. Chichester: John Wiley & Sons, Ltd.
4. 3GPP TS 23.002: Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Architecture (Release 8).
5. 3GPP TS 33.203: Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services (Release 8).
6. 3GPP TS 33.210: Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP network layer security (Release 8).
7. 3GPP TS 33.220: Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture; Generic Bootstrapping Architecture (Release 8).
8. Kent, S. & Atkinson, R. *IP Encapsulating Security Payload (ESP)*. RFC 2406, Internet Engineering Task Force, November 1998.
9. Harkins, D. & Carrel, D. *The Internet Key Exchange (IKE)*. RFC 2409, Internet Engineering Task Force, November 1998.
10. 3GPP TS 33.828: Third Generation Partnership Project; Technical Specification Group Services and System Aspects; IMS media plane security (Release 8).
11. 3GPP TS 33.106: Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Lawful Interception requirements (Release 8).
12. Chen, C.-Y., Wu, T.-Y., Huang, Y.-M. & Chao, H.-C. An efficient end-to-end security mechanism for IP multimedia subsystem. *Computer Communications* (2008), doi:10/1016/j.comcom.2008.05.025.
13. Rescorla, E. & Modadugu, N. *Datagram Transport Layer Security (DTLS).* RFC 4347, Internet Engineering Task Force, April 2006.
14. Rescorla, E. & Modadugu, N. *The Design and Implementation of Datagram TLS.* 2004.

15. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., & Schooler, E. *SIP: Session Initiation Protocol.* RFC 3261, Internet Engineering Task Force, June 2002.
16. Handley, M., Jacobson, V., & Perkins, C. *SDP: Session Description Protocol.* RFC 4566, Internet Engineering Task Force, July 2006.
17. Andreasen, F., Baugher, M., & Wing, D. *Security Description Protocol (SDP) Security Descriptions for Media Streams.* RFC 4568, Internet Engineering Task Force, July 2006.
18. Schulzrinne, H., Casner, S., Frederick, R., & Jacobson, V. *RTP: A Transport Protocol for Real-Time Applications.* RFC 3550, Internet Engineering Task Force, July 2003.
19. Baugher, M., McGrew, D., Naslund, M., Carrara, E., & Norrman, K. *The Secure Real-time Transport Protocol (SRTP).* RFC 3711, Internet Engineering Task Force, March 2004.
20. Arkko, J., Carrara, E., Lindholm, F., Naslund, M., & Norrman, K. *MIKEY: Multimedia Internet KEYing.* RFC 3830, Internet Engineering Task Force, August 2004.
21. Zimmermann, P., Johnston, A., & Callas, J. *ZRTP: Media Path Key Agreement for Secure RTP.* Internet-Draft, work in progress, June 2008.
22. McGrew, D., & Rescorla, E. *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP).* Internet-Draft, work in progress, July 2008.
23. van Gelder, A.S. (2008). *State of the art of VoIP media security.* TNO ICT report.
24. Yeh, H., Sun, H. Password authenticated key exchange protocols among diverse network domains. *Computers and Electrical Engineering 31* (3) (2005), 175-189.
25. Campbell, B., Mahy, R., & Jennings, C. *The Message Session Relay Protocol (MSRP).* RFC 4975, The Internet Engineering Task Force, September 2007.
26. Jennings, C., Mahy, R., & Roach, A. B. *Relay extensions for the Message Session Relay Protocol (MSRP).* RFC 4976, Internet Engineering Task Force, September 2007.
27. Dierks, T., & Rescorla, E. *The Transport Layer Security (TLS) Protocol Version 1.1.* RFC 4346, Internet Engineering Task Force, April 2006.
28. Eronen, P., & Tschofenig, H. *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS).* RFC 4279, Internet Engineering Task Force, December 2005.
29. Ramsdell, B. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1.* RFC 3851, Internet Engineering Task Force, July 2004.
30. zfoneproject.com (2008, October). *The Zfone Project*. http://www.zfoneproject.com

31. Wing, D. *DTLS-SRTP Key Transport draft-wing-avt-dtls-srtp-key-transport-02.* Internet-Draft, work in progress, July 2008.