Journal of Mobile Multimedia, Vol. 2, No.3 (2006) 225-258

DEVELOPMENT OF IMS PRIVACY & SECURITY MANAGEMENT FRAMEWORK FOR FOKUS OPEN IMS TESTBED

MUHAMMAD SHER THOMAS MAGEDANZ

Technical University Berlin / Fokus Fraunhofer Berlin, Germany
{sher, magedanz}@fokus.fraunhofer.de

Received March 27, 2006
Revised June 28, 2006

Privacy, confidentiality, data integrity and intrusion detection & prevention are the security methodologies to secure communication in all fields of networking, cellular and fixed communication. With the emerging of IP Multimedia Subsystem (IMS) and Next Generation Networks (NGN), there is a great need to provide secure and trusted environment to user's sensitive information and to provide measures to protect IMS operator's assets. The IMS needs powerful security association between multimedia client and the network before access is granted to multimedia services because of low security dependency of PS-domain. The security features to accomplish in securing access to the IMS are to protect SIP signalling, user authentication and authorization, development of network domain security and trusted domain using policy based security associations.

In this paper we present the security and privacy management framework for IP Multimedia Subsystem (IMS) which consists of IMS Authentication & Key Agreement (AKA), Network Domain Security, and IMS Access Security for SIP-based and HTTP-based services. The presented IMS security framework is developed for Open IMS & 3Gb Testbed of Fokus, Fraunhofer with the objective to manage security across different interfaces like air contact between user and IMS core, inter and intra domains interfaces and between IMS Core and Application Servers. It also deals with security when the user is roaming or in home network and security for UMTS access networks. This independent security framework provides additional protection against security attacks to IMS domain along with the PS (Packet Switched) domain security or IP Security.

Key words: IP Multimedia Subsystem, confidentiality, authentication, integrity protection, inter and intra domains security, Key & certificate management, HTTP & SIP security.

1. Introduction

In the prospect of global trends, the mobile communications world has defined within the evolution of cellular systems an All-IP network vision which integrates cellular networks and the Internet. This is the IP Multimedia System (IMS) [1], namely overlay architecture for the provision of multimedia services, such as VoIP and videoconferencing on top of globally emerging 3G broadband packet networks. The IMS has been standardized by 3GPP [2] and 3GPP2 [3] in the beginning of this decade and is planned for deployment in 3G wireless networks in near future. Due to the fact that IMS overlay architecture is widely abstracted from the air interfaces, the IMS can be used for any mobile access network technology as well as for fixed line access technology as currently promoted by ETSI TISPAN [4] within the NGN reference architecture definition. It is important to note that IMS defines service provision architecture, and as such can be seen as the next generation service delivery platform framework.

Security and information protection are the focal and central points for all data networks and telecommunication systems but with the emerging of fixed and mobile networks convergence like

VoIP, IPv6, WLAN, IP Multimedia System (IMS), Universal Mobile Telecommunication Systems (UMTS) and General Packet Radio System (GPRS) etc., network security becomes critical and complex to protect the networks as well as to manage secure communication between users. As we know that all IP based networks are open and distributed nature of architecture which can enable easy access to services, information, and resources, together with the constant abuse of hackers, curious individuals, fraudsters, and organized crime units. Therefore complex security techniques and mechanisms such as secure data transmission, confidentiality, authentication, data integrity, anti-replay protection and intrusion detection system are the important security consideration features for all IP networks and mobile telecommunication systems.

IMS is vulnerable to different types of attacks because users are always being connected and online and the network structure based on IP technology which is open architecture based platform. The possible reasons for passive and active attacks in IMS are due to adversary can easily access wireless link or sniffer software can be used to detect common security flaws. In order to minimize the risk of theft of information and data form hackers we have to focus an independent security framework for IMS. According to 3GPP technical specification and standardization, IMS security provides the two solutions for different level of protection:

a). *Early IMS Security Solution*:- standardized in 3GPP Release 5 with limited security functionality and aiming to protect early IMS deployment and offer less security. It provides authentication of subscribers for services access and identity confidentiality on the radio interface. It also provides radio interface encryption.

b). *Complete IMS Security Solution*:- standardized in 3GPP Release 6 with full security functionality and it builds on the early security solutions with objective to improve it. It offers new security features and secures new services to protect network and terminals with data protection.

The article is organised as: next part discusses IMS as a future fixed mobile convergence; section 3 is about IMS security attacks and objectives. In sections 4, 5 and 6, we will discus IMS security framework architecture, Authentication and Key Agreement and protection of air link between user and IMS core network respectively. Section 7 describes inter and intra-domains security architecture and section 8 explains security for HTTP based services. Section 9 is about Fokus IMS Testbed and last section concludes and discusses about the future work.

2. IMS – the Future Fixed-Mobile Convergence Technology

The 3GPP Release 5 [2] defines IP Multimedia Systems specifications architecture on top of packet switched core network (PS CN) for the provision of real time multimedia services. The IMS provides easy and efficient ways to integrate different services, even from third parties and enables the seamless integration of legacy services and is designed for consistent interactions with circuit switched domains. The IMS manages event oriented quality of service policies e.g. use of VoIP and HTTP in a single session: VoIP has QoS, HTTP is best effort. These systems (IMSs) also have event oriented charging mechanism policies; means change specific events on the appropriate level. If two events need the same IP resources we may charge them differentially for the same user in the same session. These characteristics make the IMS as the future technology in a comprehensive service and application oriented network.

The IMS is based on the principles and protocols of the Internet defined by the IETF, which have been adapted for their use within a secure, scalable carrier grade environment. The Session Initiation Protocol (SIP) [5] is used as the standard signalling protocol that establishes controls, modifies and

terminates voice, video and messaging sessions between two or more participants. The Call State Control Functions (CSCF) server implements and manages the SIP functionalities. The Authentication, Authorization and Accounting (AAA) related functionality provision within the IMS is based on the Diameter protocol [6] and is implemented in the Home Subscriber Server (HSS). Media Gateways and Media Server support potentially required adaptation of multimedia information for specific QoS requirements. IMS layered architecture consists of three planes as shown in figure 1: the user, control, and application planes. In spite of the fact that IMS was initially designed (in release 5) for cellular IP networks (GPRS and UMTS), all access-specific issues have been separated in the last release (release 6) from the IMS core. This means that transport and bearer services representing the user plane are separated form signalling network and session handling services representing the control plane.

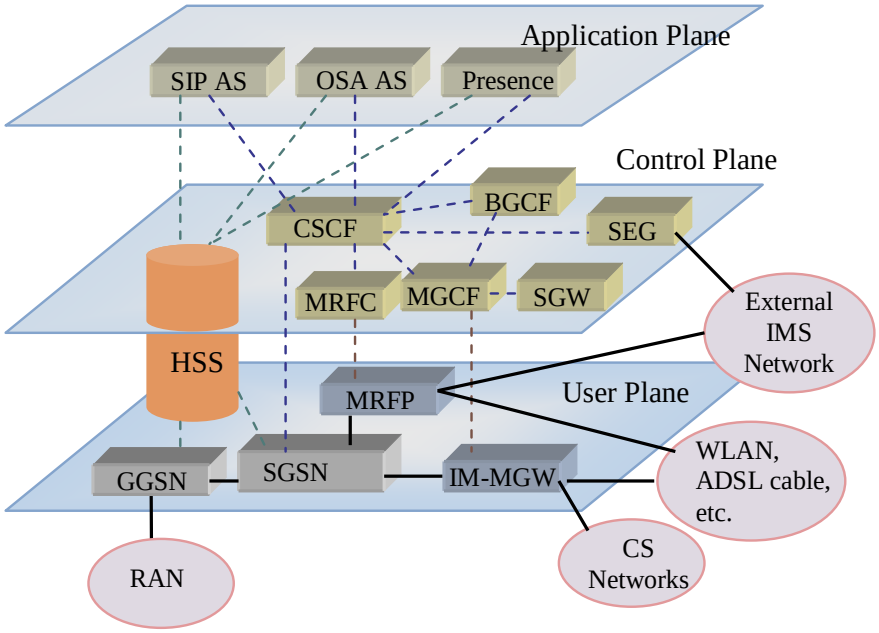

Figure 1 IMS Layered Architecture

2.1 IMS Components and Entities

IMS consists of different entities with well-defined functions. These entities can be roughly classified into six main categories [7]: session handling and routing (CSCF), database (HSS, SLF), inter-working elements (BGCF, MGCF, IM-MGW, and SGW), services (application server, MRFC, MRFP), support entities (PDF), and charging. Between each of these entities the standards define a reference point, which describes the functionalities (e.g. how the application server can obtain user location from the HSS) and the used protocol. The important components of IMS (shown in figure 2) are given as:

- **P-CSCF** (Proxy Call State/Session Control Function):- It behaves like a proxy accepting requests and services. It is the first contact point within the IP Multimedia Core Network subsystem. Its address is discovered by UEs following Packet Data Protocol (PDP) context activation. Performed functions are: Authorize the bearer resources for the appropriate QoS level, emergency calls, monitoring, header (de)compression and identification of I-CSCF.

- **I-CSCF** (Interrogating Call State Control Function):- It assigns S-CSCF to a user performing SIP registration, charging and resource utilization. It is the contact point within an operator's network for all connections destined to a subscriber of that network operator, or a roaming subscriber currently located within that network operator's service area. There may be multiple I-CSCFs within an operator's network. Performed functions are: Assigning an S-CSCF to a user performing SIP registration / Charging and resource utilisation: generation of Charging Data Records (CDRs) / acting as a Topology Hiding Inter-working Gateway (THIG).
- **S-CSCF** (Serving Call State Control Function):- It performs the session control services for the endpoint and maintains session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionality. Performed functions are: User Registration / Interaction with Services Platforms for the support of Services. The S-CSCF decides whether an Application Server is required to receive information related to an incoming SIP session request to ensure appropriate service handling. The decision at the S-CSCF is based on filter information received from the HSS. This filter information is stored and conveyed on a per application server basis for each user
- **MRF** (Media Resource Function):- It provides media stream processing like media mixing, media announcements, media analysis and media transcoding. The Media Resource Function (MRF) can be split up into the Media Resource Function Controller (MRFC) and the Media resource Function Processor (MRFP). The triple of Border Gateway Control Function (BGCF), Media Gate Control Function (MGCF) and Media Gate (MG) perform the bearer interworking between RTP/IP and the bearers used in the legacy networks.
- **HSS** (Home Subscription Function):- It is the master database of an IMS that stores IMS user profiles including individual filtering information, user status information and application server profiles. HSS is the equivalent of the HLR (Home Location Register) in 2G systems; however, extended with two Diameter based reference points.
- **AS** (Application Server):- It provides service platform in IMS environment. It does not address how multimedia/value added applications are programmed but only well defined signaling and administration interfaces (ISC and Sh) and SIP and Diameter protocols are supported. This enable developers to use almost any programming paradigm within a SIP AS, such as legacy Intelligent Network servers (i.e. CAMEL Support Environments), OSA/Parlay servers/gateways, or any proven VoIP SIP programming paradigm, like SIP Servlets, call programming language (CPL) and Common Gateway Interface (CGI) scripts, etc. The SIP AS is triggered by the S-CSCF which redirects certain sessions to the SIP AS based on the downloaded filter criteria or by requesting filter information from the HSS in a user based paradigm. The SIP AS itself comprises filter rules to decide which of the applications deployed on the server should be selected for handling the session. During execution of service logic it is also possible for the SIP AS to communicate with the HSS to get additional information about a subscriber or to be notified about changes in the profile of the subscriber.

2.2 IMS Reference Points and Interfaces

To connect different IMS entities with each other and carrying signal and information, interfaces and reference points are defined by 3GPP. We will discuss only those interfaces where information are necessary to protect.

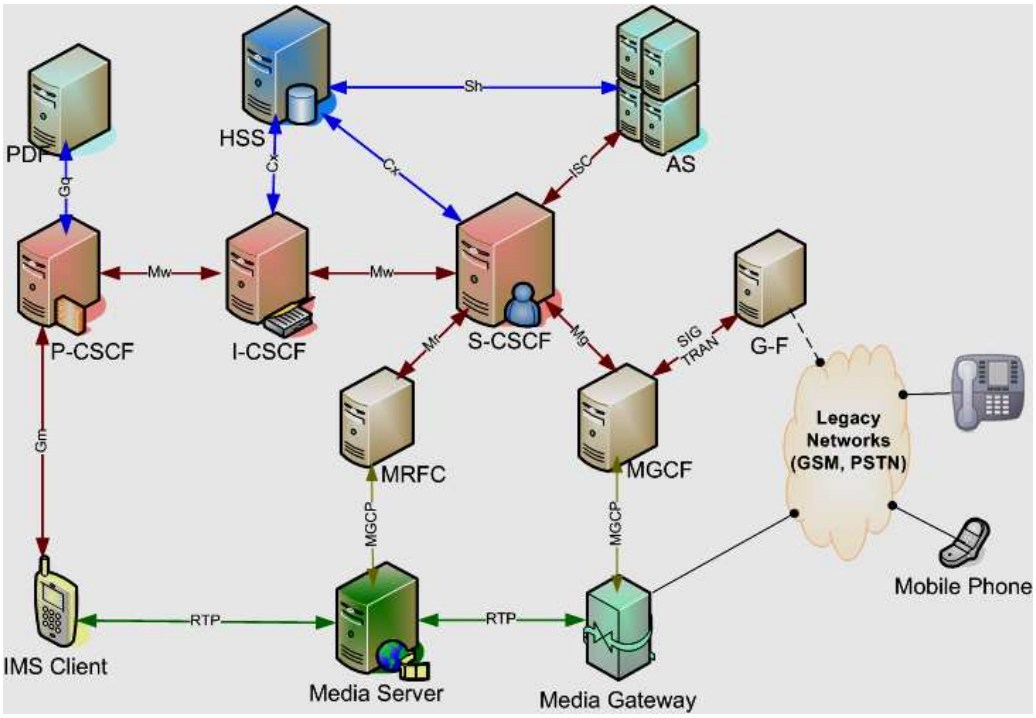

Figure 2 IMS Entities and Interfaces

- **Gm** Interface: It connects the UE to the IMS Core Network. It is used to transport all SIP signalling messages between the UE and the P-CSCF. Procedures in the Gm reference point can be divided into three main categories: registration, session control and transactions.
- **Cx**: This reference point is between HSS and the CSCF. Subscriber and service data are permanently stored in the HSS. This centralized data is utilized by the I-CSCF and the S-CSCF when the user registers or receives sessions using Cx reference point and the selected protocol is Diameter. The procedure can be divided into three main categories: location management, user data handling and user authentication.
- **ISC**: The IMS Service Control interface is between the S-CSCF and the application server. The AS could behave as an SIP UA or SIP Proxy on this interface. The S-CSCF process the received SIP messages based on the filter criteria stored in the user profile obtained from the HSS.
- **Sh**: It connects the AS with the HSS and the used protocol is Diameter. It enables the AS to obtain user data or to get to know the S-CSCF to send SIP request.
- **Ut** Interface: It is between the user equipment and the AS. HTTP is the chosen data protocol and any further communication protocol needed between user and application has to rely on HTTP.
- **Mw**: It is the reference point between different CSCFs i.e. between P-CSCF and I-CSCF & S-CSCF. The procedures in the Mw reference point can also be divided into three main categories: registration, session control and transactions.

3. Different Attacks Possibilities on IMS and Security Features

Now we will try to explore different security attacks and threats to IMS domain and than discuss the features of security framework.

3.1 Security Attacks and Threats to IMS

The possible attacks on IMS are classified as:

- **ISIM Cloning**:- The process of changing the identity of one entity to that of an entity of the same type, so that there are two entities of the same type with the same identity. ISIM can be cloned be extracting the secret key K and IMSI from one ISIM and shifting to another ISIM using different attack techniques.
- **Denial-of-Services (DoS) Attack**:- Jamming of radio signal and flooding by authentication requests to P-CSCF and others devices.
- **Spoofing Attack**:- The malicious node hides its presence in the network and intercepts traffic and attackers temper with messages. These nodes become trusted node in IMS.
- **Man-in-the-Middle Attack**:- The hackers search the breaches and break the authentication process and integrity protection process in order to get the IMS services for free.
- **Impersonation**:- Impersonating a server causes to misroute the messages. The existing authentication processes are unable to identify between the intruder and legitimate user. This way the attacker has free access to IMS services and the victim get charged for the attacker's usage of services
- **Eavesdropping**:- Hackers get session information if messages are sent in clear text and can easily launch variety of hijacking attacks from session information.
- **Session Hijacking**:- With INVITE request it is possible to direct media elsewhere and with 3XX-Class Response to redirect session establishment request to the hijacker's machine
- **Repudiation:**- User or network denies actions that have taken place. Non-repudiation is a security service which counters the treats of repudiation.
- **Masquerading**:- Intruder hoaxes as authorized user to get confidential information and to get system services.

3.2 Objective and Features of IMS Security Framework

Different features and objectives of developing security framework for IP Multimedia Subsystem (IMS) are summarized as:

- **Confidentiality**: To ensure that the information is adequately protected against misuse i.e. data is strictly limited to authorized partners and the resources and services provided by network operators are adequately protected. Possibility for IMS specific confidentiality protection shall be provided to SIP signalling messages between the UE and the P-CSCF. Mobile Operators shall take care that the deployed confidentiality protection solution and roaming agreements fulfils the confidentiality requirements presented in the local privacy legislation [16].
- **Integrity**: To ensure that data and information are unchanged and identified with respect to their origins. Integrity protection shall be applied between the UE and the P-CSCF for protecting the SIP signalling.
- **Accountability**: To ensure that identity of all users can be guaranteed.
- **Availability**: To ensure that services are correctly provided and are available.

- **Accessibility**: To ensure that only authorized entities may have access to sensitive data.
- **Interoperability**: To ensure that security features like interoperability and roaming between different serving networks are standardized world-wide.
- **Network Topology Hiding:** The operational details of an operator's network are sensitive business information that operators are reluctant to share with their competitors. While there may be situations (partnerships or other business relations) where the sharing of such information is appropriate, the possibility should exist for an operator to determine whether or not the internals of its network need to be hidden. It shall be possible to hide network topology from other operators, which includes hiding of number of S-CSCFs, capabilities of S-CSCFs and capability of the network. The I-CSCF shall have the capability to encrypt the address of an S-CSCF in SIP Via, Record-Route, Route and Path headers and then decrypt the address when handling the response to a request. The P-CSCF may receive routing information that is encrypted but the P-CSCF will not have the key to decrypt this information. The mechanism shall support the scenario that different I-CSCFs in the HN may encrypt and decrypt the address of the S-CSCFs [16].
- **SIP Privacy Handling in IMS Networks:** Privacy may in many instances be equivalent with confidentiality i.e. to hide information (using encryption) from all entities except those who are authorized to understand the information. The SIP Privacy Extensions for IMS Networks do not provide such confidentiality. The purpose of the mechanism is rather to give an IMS subscriber the possibility to withhold certain identity information of subscriber [16].

4. IMS Security Architecture

As we know that 3 GPP specifies two security solutions for IMS i.e. early IMS security solution and full IMS security solution. In the early IMS security solution (standardized in 3GPP 5) it is assumed that the user is authenticated on GPRS level and IMS can reuse this authentication. It means that there is no IPSec connection between UE and P-CSCF and there exist no IMS AKA and HTTP Digest authentication. The HSS binds the IMSI and MSIDN to the user private and public identities and GGSN prevents the source IP spoofing. The full IMS security IMS solution (standardized in 3GPP 6) is divided in two groups i.e. network domain security which is related to existing GPRS security and access domain security that defines SIP security that is implemented on hop-by-hop fashion and end-to-end security is not supported.

The overall security for IP Multimedia System (IMS) [1] as standardized by 3GPP [2] in its different releases is summarized in diagram 3 and involves following procedures and recommendations:

- Authentication & Key Agreement between IM subscriber and home network
- Security Mechanism Agreement between IM client and visited network
- Integrity Protection and Confidentiality
- Network Domain Security between different Domains
- Existing GPRS/UMTS Access Security

The proposed architecture of IMS security management framework for IMS Fokus Fraunhofer Testbed consists of seven security associations and agreements [8] (shown in figure 4) that are mandatory to protect IMS environment for secure and safe communication over wireless and wireline networks including circuit switched (CS) domain as well as packet switched (PS) domain.

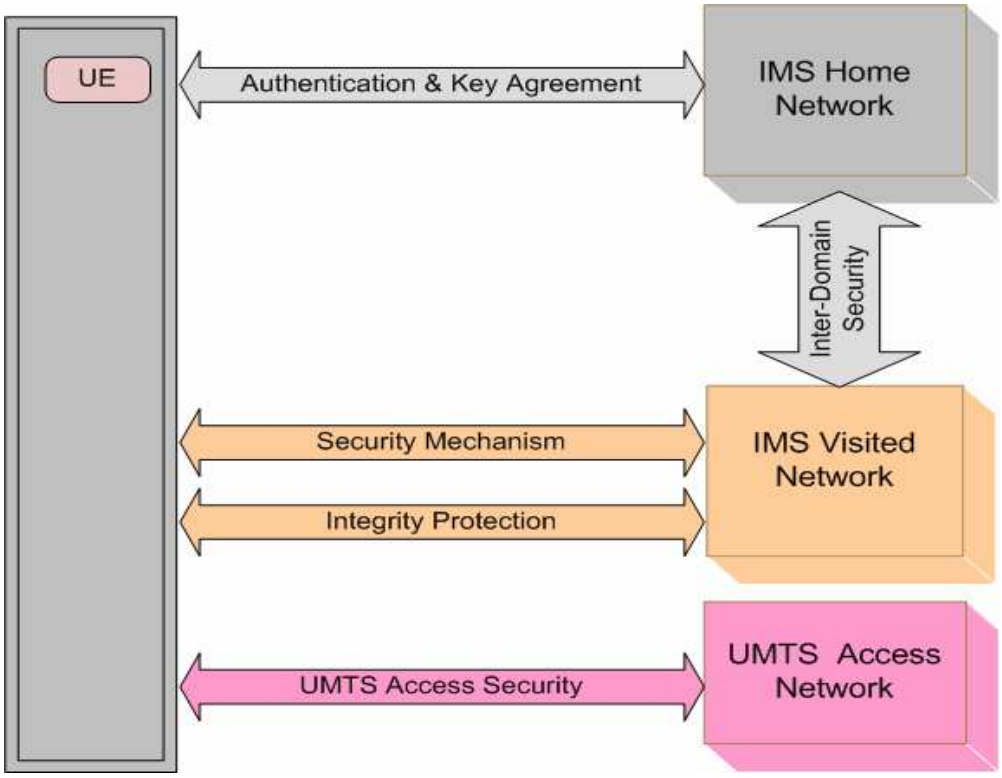

Figure 3 Overall IMS Security

- **SA1**: It provides mutual authentication of user and network. The HSS is responsible for generating keys and challenges and than delegate's subscriber authentication to Serving-CSCF (S-CSCF). The long-term key in ISIM and HSS is associated with the IMPI. The detailed process will be explained in section 5.
- **SA2**: It provides a secure link and a security association between UE and Proxy-CSCF (P-CSCF) for protecting of Gm reference point (air contact). In IMS, NDS/IP is used to protect SIP signaling, but SIP communication at Gm interface between UE and P-CSCF is outside the scope of NDS/IP and needs additional measures for security. It will be explained in section 6.
- **SA3**: It provides security within network domain internally for Cx-interface. Home Subscriber Server (HSS) stores subscriber and service data permanently and this centralized data is utilized by I-CSCF and S-CSCF when the user registers or receives sessions through Cx interface and the selected management protocol is Diameter. Diameter messages over Cx and Dx interfaces make use of Stream Control Transmission Protocol (SCTP) [9] with IPSec for secure communication.
- **SA4**: It provides security between different networks for SIP capable nodes and only applicable when P-CSCF resides in visited network i.e. user is roaming. When P-CSCF resides in visited network than by virtue of AKA protocol, the shared secret is only accessible in home network, which means that while authentication needs to take place in visited network, certain delegation of responsibility needs to be assigned to P-CSCF, as IPSec SAs exist between P-CSCF and UE.

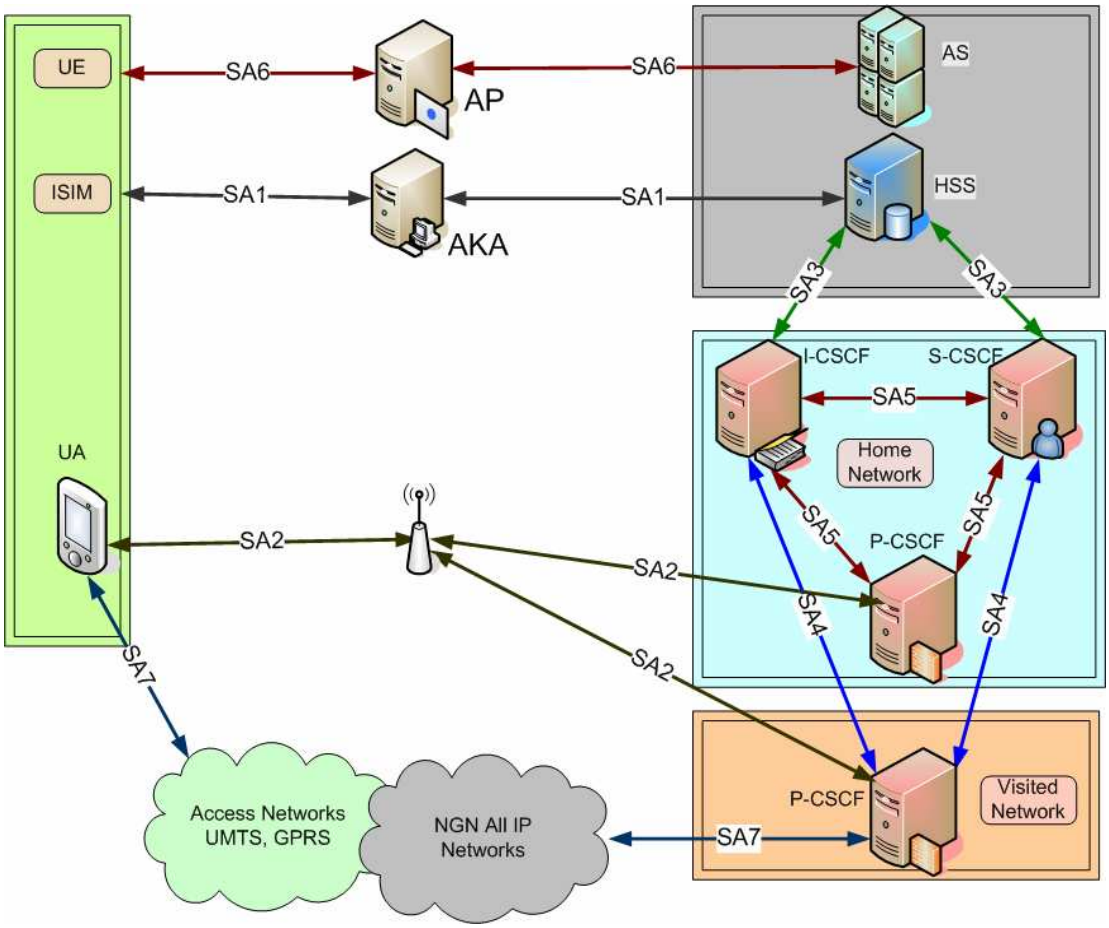

Figure 4 IMS Security Architecture

- **SA5**: It provides security within network internally between SIP capable nodes and also applies when P-CSCF resides in home network. The IMS protects all IP traffic in core network using Network Domain Security/IP (NDS/IP) [10] which provides confidentially, data integrity, authentication and anti-replay protection for traffic using combination of cryptographic security mechanisms and protocol security mechanisms applied is IP Security (IPSec). The security procedure for SA4 and SA5 will be explained in section 7.
- **SA6**: The protocols working across Ut interface performs functionality to manage data traffic for HTTP based applications. Thus securing Ut interface means to achieve confidentiality and data integrity protection of HTTP-based traffic [11]. The authentication and key agreement for Ut interface is also based on AKA which generates session keys. The IMS defines Generic Bootstrapping Architecture (GBA) [12] which is utilizes Generic Authentication Architecture (GAA) [13] that performs mutual authentication before accessing services. The authentication in the Ut interface is performed by authentication proxy. Traffic in the Ut interface goes through the authentication proxy and is secured using the bootstrapped session key. The Ut interface employs the Transport Layer Security (TLS) for both confidentiality and integrity protection. We will discuss the detail procedure in section 8.

- **SA7**: It manages to protect user and user's information on access networks e.g. UMTS, GSM, GPRS, WLAN, DSL and VoIP. The security association takes place independently either in CS service domain or PS service domain. For UMTS access network, security management architecture consists of User Service Identity Module (USIM), Mobile Equipment (ME), Access Network (AN), Service Network (SN) and Home Environment (HE) [14]. USIM is required for accessing Packet Switched (PS) domain in General Packet Radio System (GPRS) and identifies particular subscriber. USIM contains security parameters for accessing PS-domain, International Mobile Subscriber Identity (IMSI), list of allowed access points, MMS-related information. In serving network, the Serving GPRS Support Node (SGSN) links Radio Access Network (RAN) to packet core network in the PS-service domain. It is responsible for performing both control and traffic handling functions for PS domain. The control parts deal with mobility management and session management. The SGSN also ensures appropriate QoS and generates charging information. In CS-service domain, the related part is Visitor Location Register (VLR). The authentication and key agreement procedure involves Authentication Centre (AUC) within HE, SGSN or VLR and Mobile Station (MS) networks entities. The detailed architecture is explained in our paper [15].

5. IMS Authentication & Key Agreement (AKA) Procedure

In order to get IP Multimedia Services, user's one public identity which is called IP Multimedia Public Identity (IMPU) needs to be registered and user's private identity which is called IP Multimedia Private Identity (IMPI) has to be authenticated by IMS. Authentication for IMS access is based on the Authentication and Key Agreement (AKA) protocol. The Secret Key (K) and AKA algorithms are stored in IP Multimedia Services Identity Module (ISIM) which is normally embedded on Universal Integrated Circuit Card (UICC) like a smart card based device. The IMS security is based on a long-term secret key (K) shared between ISIM and Home Network (HN) Authentication Centre (AUC). The AKA performs mutual authentication of ISIM and AUC, and generates Cipher Key (CK) and Integrity Key (IK) [16].

In the following we will only consider IMS AKA procedure for unregistered IP Multimedia client and successful mutual authentication with no synchronization error. For authentication purpose, the client sends SIP Register request to S-CSCF via P-CSCF and I-CSCF for authentication purpose. This request contains User Private Identity (IMPI) and User Public Identity (IMPU). After receiving this request, the S-CSCF sends Authentication Vector Request (AV-Req (IMPI, m)) to Home Subscriber Server (HSS) for getting AV vector and HSS generates and sends an n-ordered array of AVs to S-CSCF and sequence number in AV-Req-Response. Each AV consists of CK, IK, RAND and XRES and AUTHN as given in eq.1.

$$AV = RAND||AUTN||XRES||CK||IK \quad (1)$$

One AV is required for one authentication and is selected on first-in/first-out basis. The S-CSCF sends SIP authentication challenge (Auth-Challenge) to P-CSCF via I-CSCF and the P-CSCF stores the keys (IK, CK) and forward the remaining message (Auth-Challenge (IMPI, RAND, AUTN)) to the client. The network starts authentication procedure by using authentication request that contains a random challenge (RAND) and authentication token (AUTN). The AUTN is calculated as:

$$AUTN = SQN + AK \parallel AMF \parallel MAC \quad (2)$$

where SQN is sequence number, $\parallel$ is XOR addition & AMP is an authentication and key management field.

$AK = F5_K(RAND)$; F5 is a key generating function.

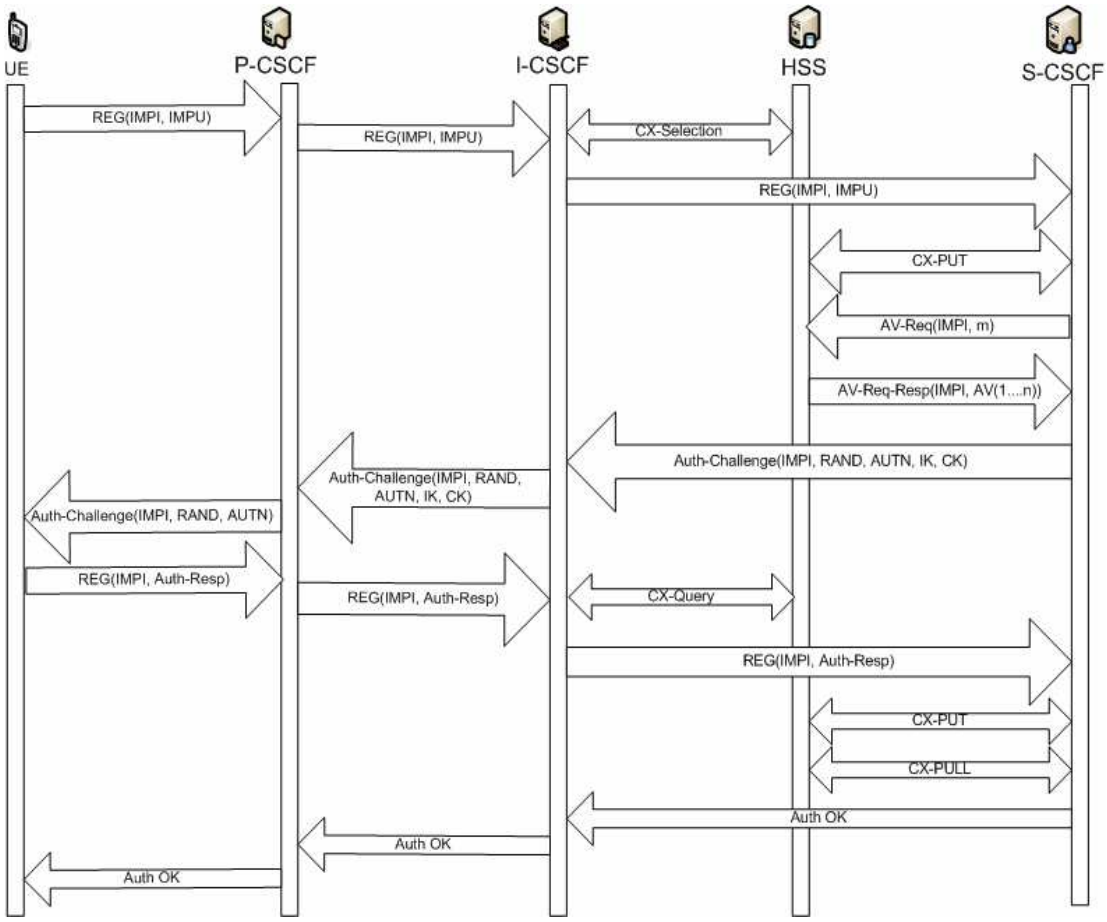

Figure 5 IMS Authentication Process

Upon receiving challenge, the client takes AUTN which includes MAC and SQN. The client calculates XMAC as given in eq. 3, and verify that XMAC = MAC and SQN in correct range.

$$XMAC = F1_K\,(SQN \,\|\, RAN \,\|\, AMF) \tag{3}$$

If both are ok, client calculates Auth-Response including RES and some other parameters and sends back to P-CSCF as REG (IMPI, Auth-Response) message. The client also calculates the CK and IK keys at this stage as given in equation 4.

$$CK = F3_K(RAND)\ \&\ \ IK = F4_K\,(RAND) \tag{4}$$

Where F3, F4 are key generating functions and RAND is a random value.

The P-CSCF forwards this response to I-CSCF which quires the HSS to find the address of S-CSCF and the I-CSCF forwards this response to the S-CSCF. The S-CSCF retrieves XRES from the Response and compare with RES which is sent to the user as mentioned in RFC 3310 [17]. If verification is successful the client has been authenticated and public identity (IMPU) is registered in the S-CSCF. The complete procedure is explained in figure 5.

The ISIM verifies the AUTN for network authenticity. The ISIM and the HSS keep track of sequence numbers SQN_{ISIM} and SQN_{HSS} respectively for each round of authentication procedures. If

the ISIM detects an authentication whose sequence number is out of range, then it aborts the authentication and reports back to network with a synchronization failure message, including with correct sequence number [16]. This technique is used to provide for anti-replay protection. The ISIM produce authentication response (RES) as in eq.5 from secret key and random challenge (RAND) in respond to network's authentication request.

$$RES = F2_K\ (RAND) \tag{5}$$

where F2 is a message authentication function.

By this process the UE and home network have successfully authenticated and establishes a secure communication channel. The device on which ISIM resides is a temper-resistant and only physical access to it is not sufficient to result in exposing the secret key. It is further protected by the PIN code from unauthorized access. Thus combination of ownership of physical device USIM/ISIM and knowledge of secret pin code makes the security architecture of IMS more robust [7].

6. Protection of Air Contact (Gm Interface) between User and IMS Core Network

The Gm reference point connects User to IP Multimedia System Core. It is used to transport all Session Initiation Protocol (SIP) [5] signalling messages between UE and P-CSCF. The protection of this interface is very essential and therefore its security is considered very important. In IMS, NDS/IP is used to protect SIP signalling, but SIP communication at Gm interface between UE and P-CSCF is outside the scope of NDS/IP and needs additional measures for security. The IMS in 3GPP Releases 5 and 6 makes use of IPSec as the security mechanism between P-CSCF and the UE. The Internet Protocol Security (IPSec) [18] is only one of several possible security mechanisms. The IMS was designed to allow alternative security mechanisms over the Gm interface as well. Allowing such openness usually creates backward compatibility problems because, for example, a Release 6-compliant UE would not be able to understand any alternative security mechanism, while it could be attached to P-CSCF of higher release that would already support alternatives to IPSec [7]. Therefore, the SIP Security Mechanism Agreement (Sip-Sec-Agree) [19] was introduced to allow UE and P-CSCF to negotiate a common security mechanism for use between them. For current releases the only security mechanism is IPSec; however, it might be that some entities already support alternative mechanisms on proprietary basis.

During authentication of user, UE and IMS also negotiate security mechanisms for securing subsequent SIP traffic in Gm interface. SIP protocol is used for this security agreement and the UE and P-CSCF exchange their respective lists of supported security mechanisms and the highest commonly supported one is selected to provide data integrity protection. Once the security mechanism has been selected and its use started, previously exchanged list is replayed back to network in a secure fashion. This helps network to verify that the security mechanism selection was correct and the security agreement was not tampered with. An example of an attack that would be possible without this feature is bidding-down attack, where an attacker forces peers into selecting a known weak security mechanism. The IPsec ESP [20] provides both confidentially as well as data integrity and authentication which are mandatory in IMS access security. AKA session keys are used as keys for the ESP SAs i.e. IK is used as authentication key, and CK as encryption key. The AKA Protocol cannot run directly over IP and requires a vehicle to carry protocol messages between the UE and the home network. The SIP acts as vehicle for AKA protocol and it is tunnelled inside SIP and therefore IMS access is obviously to authenticate it.

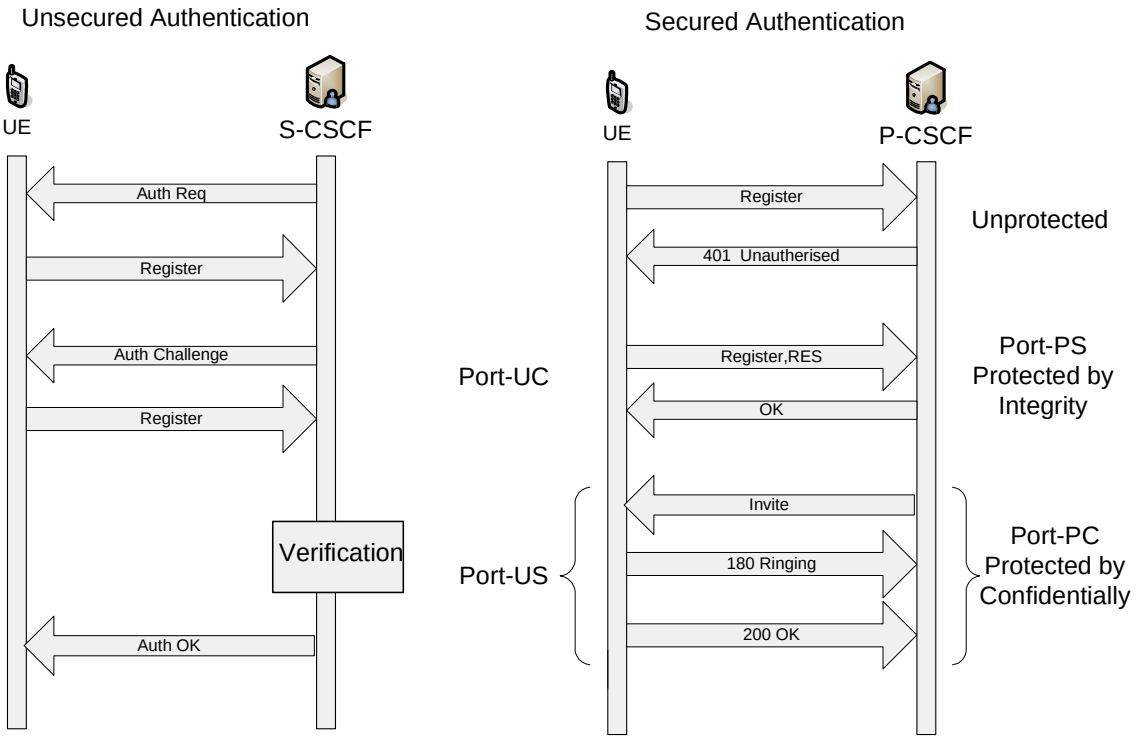

Figure 6 Unsecured and Secured User's Authentication

6.1 Use of IPSec ESP for SIP Confidentiality Integrity Protection

In order to provide the SIP Integrity protection between UE and P-CSCF, the recommended protocol is IPSec ESP (IP Security Encapsulated Security Payload) [20] which protect all SIP signalling messages at IP layer. The use of ESP for integrity protection will be applied in transport mode as shown in figure 7. In this mode TCP header, payload and padding fields are encrypted in IP packet and new ESP header which contains information like Security Parameter Index (SPI), is added between IP header and encrypted data. Finally MAC is calculated on all the data except IP header. The receiver checks integrity protection by calculating MAC and comparing with received MAC. The integrity algorithm is either Hash Message Authentication Code – Message Digest (HMAC-MD5-96) [21] or Secure Hash Algorithm (HMAC-SHA-1-96) [22]. If the selected algorithm is HMAC-MD5-96 than integrity key (IK_{ESP}) is calculated as follows which is 128 bits.

$$IK_{ESP} = IK_{IM} \tag{6}$$

But for other algorithm (HMAC-SHA-1-96), integrity key (IK_{ESP}) is calculated as follows to create a 160 bits key.

$$IK_{ESP} = IK_{IM} \parallel 32 \text{ bits zeros string} \tag{7}$$

In order to provide confidentiality to SIP signalling on air interface, UE and P-CSCF agree on the specific encryption algorithm, mechanism and encryption key. The IPSec ESP [20] in transport is recommended by 3GPP to provide confidentially protection of SIP signalling at Gm interface between IMS core and IMS client. The encryption algorithm is either Data Encryption Standard- Triple DES used in Cipher Block Code (DES-EDE3-CBC) [23] or Advance Encryption Standard in Cipher Block

Code (AES-CBC) [24] with 128 bit key. The encryption key (CK_{ESP}) for DES-EDE3-CBC is calculated as:

$$CK_{ESP} = CK_{IM1} \parallel CK_{IM2} \parallel CK_{IM1} \quad (8)$$

Where CK_{IM1} (64 bits) and CK_{IM2} (64 bits) are derived from CK_{IM} (128 bits) as

$$CK_{IM} = CK_{IM1} \parallel CK_{IM2} \quad (9)$$

If the selected algorithm is AES-CBC, then encryption key (CK_{ESP}) is as: $K_{ESP} = CK_{IM}$

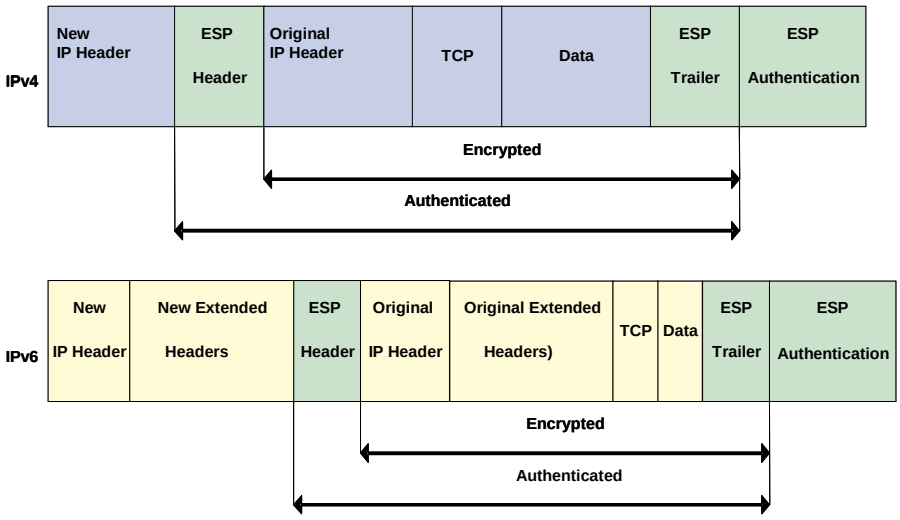

Figure 7 ESP Header Format

6.2 SIP Integrity and Confidentiality Procedure

Now we discuss the procedure to set-up security associations between client (UE) and P-CSCF for the protection of Gm interface. The client sends security-setup message in the REG (Sec-Setup = SPI-U, Port-U, UE I & E Algorithms List) message as shown in figure 8.

Where

SPI-U = (SPI-UC, SPI-US); pair of Security Parameter Index values that client selects.

Port-U = (Port-UC, Port-US); pair of protected ports numbers of clients and server.

UE I&E Algos List = List of Integrity and Encryp Algos Identifiers that client supports.

Upon receipt of this message, P-CSCF stores security parameters along with client's IMPI, IMPU and IP address and adds keys IK_{IM} and CK_{IM} received from S-CSCF. Next the P-CSCF sends Auth-Challenge (Sec-Setup = SPI-P, Port-P,P-CSCF I & E Algorithms List) to client.

Where

SPI-P = (SPI-PC, SPI-PS); pair of Security Parameter Index values that P-CSCF selects.

Port-P = (Port-PC, Port-PS); pair of protected ports numbers of clients and server.

P-CSCF I&E Algos List = List of Integrity and Encryp Algos Identifiers that P-CSCF supports.

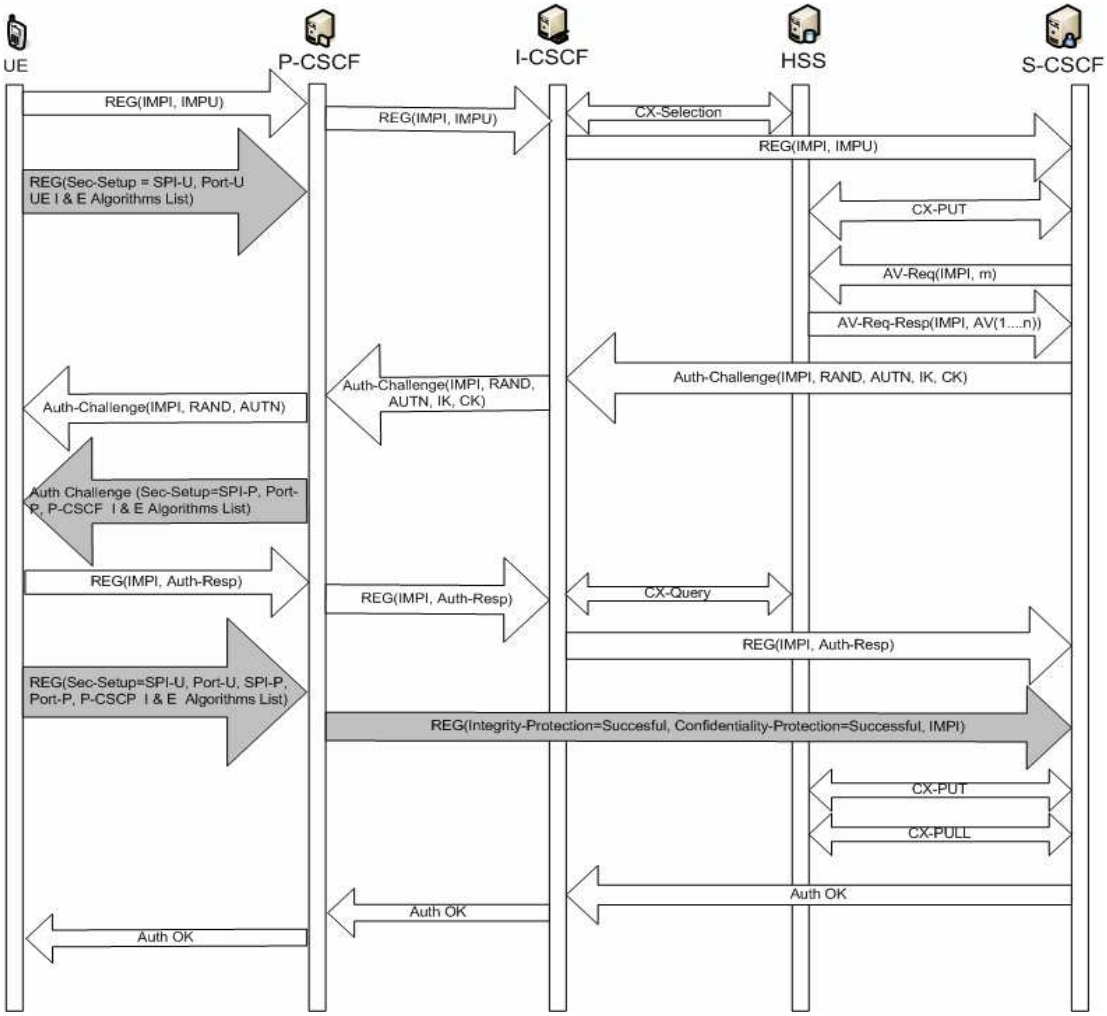

Figure 8 Authentication with Integrity and Confidentiality Protection

The client then sends final security setup message as REG (Sec-Setup = SPI-U, Port-U, SPI-*P*, Port-*P*, *P-CSCF* I & E Algorithms Lis*t*) to P-CSCF and it checks whether these parameters are same. If they match registration is successful. Finally P-CSCF sends REG (Integrity-Protection=Successful, Confidentiality-Protection=Successful, IMPI) to S-CSCF to inform that client messages are integrity and confidentiality protected [16].

7. IMS Inter & Intra-Domains Security Architecture

IP Multimedia System supports communication between home network and visited network, creating two scenarios weather IMS terminal is in home network or roaming. In first scenario UE's first point of contact to IMS, called P-CSCF is located in home network and in the second scenario the P-CSCF is located in visited network (roaming). The traffic between the visited and home network are protected using Network Domain Security/Internet Protocol (NDS/IP) at IP layer. The NDS/IP only protects traffic between network elements in IP layer.

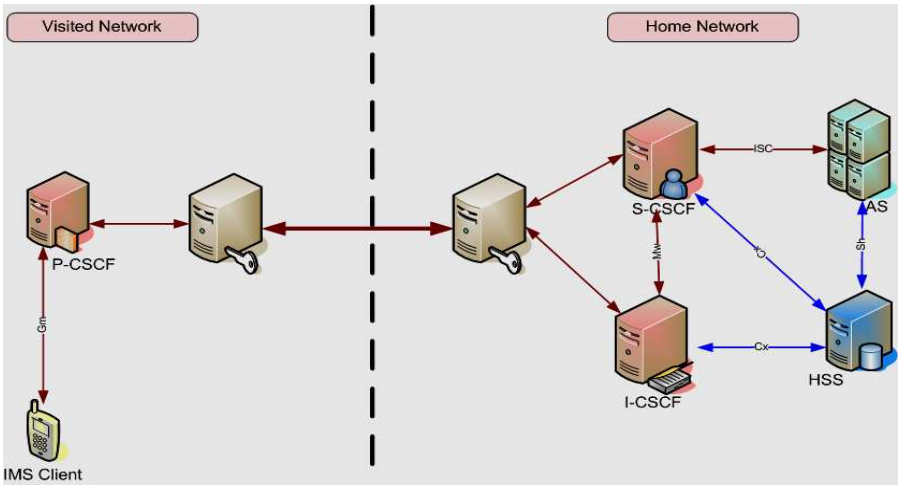

Figure 9 IMS Roaming User

A security domain is a network operated by a single administrative authority that implements a uniform security policy within that domain. As a result the level of security will be the same within a security domain. Mostly the security domain is related directly to an operator's core network but it is however possible to run several security domains making subset of operator's entire core network. IMS protects all IP traffic in the core network using NDS/IP which provides confidentially, data integrity, authentication and anti-replay protection for traffic using combination of cryptographic security mechanisms and protocol security mechanisms applied in IP security (IPsec). In NDS/IP platform the interfaces between elements inside security domain are denoted by Zb and interfaces between different security domains are denoted by Za as shown in figure 10. Use of Za interface is always mandatory between different security domains while use of Zb interface is optional and up to the security domain's administrator. Data authentication and integrity is mandatory for both interfaces, while use of encryption is recommended for Za and optional for Zb.

The NDS/IP is used to protect operators IMS Core Network as well as traffic between visited and home network. The fundamental idea of NDS/IP architecture is to provide hop-by-hop security, according to the *chained-tunnels* or *hub-and-spoke* models of operation. And utilizing hop-by-hop security also makes it easy to maintain separate security policies internally, and towards other external security domains. The Network Entities (NEs) establish and maintain ESP (Encapsulated Security Payload) Security Associations (SAs) as needed towards a SEG (Security Gateway) or other NEs within the same security domain. All NDS/IP traffic from NE in one security domain towards NE in other security domain is routed via SEG, and will receive hop-by-hop security protection towards the final destination [16].

The operators may decide to establish only one ESP Security Association between two communicating security domains, which will lead to coarse-grained security granularity. This has a benefit that a certain measure of protection against traffic flow analysis is given. But the disadvantage is that it is not possible to differentiate the security protection provided between the communicating entities. This does not preclude negotiation of finer grained security granularity at the discretion of the communicating entities.

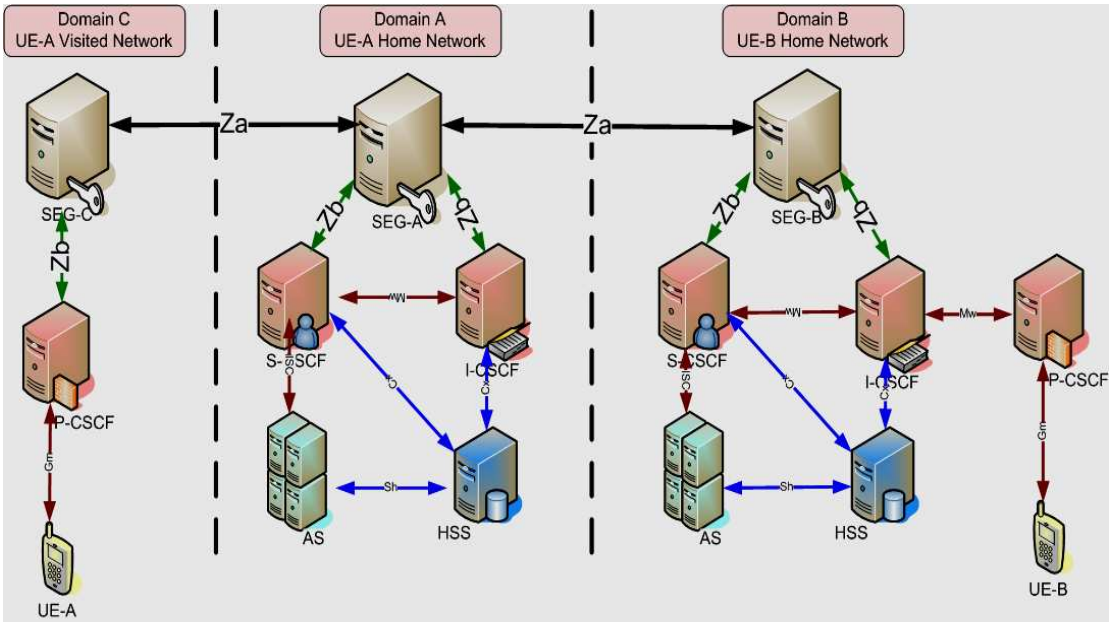

Figure 10 Visited and Home Network Scenarios

7.1 IMS Security Gateways

The data traffic entering and leaving a security domain passes through a security gateway (SEG) which is an entity on the border of IP security domains, providing security to IP based protocols. The SEGs establish communication over Za-interface, which is located between SEGs from different IP security domains. All NDS/IP traffic passes through SEG before entering or leaving the security domain. A security domain can have more than one SEG and each SEG is defined to handle NDS/IP traffic in or out of the security domain towards well-defined set of reachable IP security domains. When protecting inter-domain IMS traffic it is mandatory to provide confidentiality, data integrity, and authentication in NDS/IP [7].

The SEGs establish and maintain an IPSec secured ESP security association in tunnel mode between security domains. The SEG will normally provide at least one IPSec tunnel at all times to a particular peer SEG. The SEG will maintain logically separate Security Associations Database (SAD) and Security Policy Database (SPD) databases for each interface [25]. Each SEG is responsible for setting up and maintaining IPSec security associations (SAs) [18] with its peer SEGs. These SAs are negotiated using Internet Key Exchange (IKE) [26] protocol, where authentication is done using long term keys stored in the SEGs. A total of two SAs per peer connection are maintained by the SEG; one for inbound traffic and one for outbound traffic. In addition, the SEG maintains a single Internet Security Association and Key Management Protocol (ISAKMP) SA [27], which is related to key management and used to build up actual IPSec SAs between peer hosts. One of the key prerequisites for ISAKMP SA is that the peers are authenticated. In NDS/IP, authentication is based on pre-shared secrets. The number of SEGs in a security domain depends on the need to differentiate between the externally reachable destinations, need to balance the traffic load, and to avoid single points of failure. The security gateways enforce security policies for interworking between networks. The security may include filtering policies as well as firewall functionality. The SEGs are responsible for security

sensitive operations and need to be physically secured. Also, provision must be made for the secure storage of long-term keys used for IKE authentication.

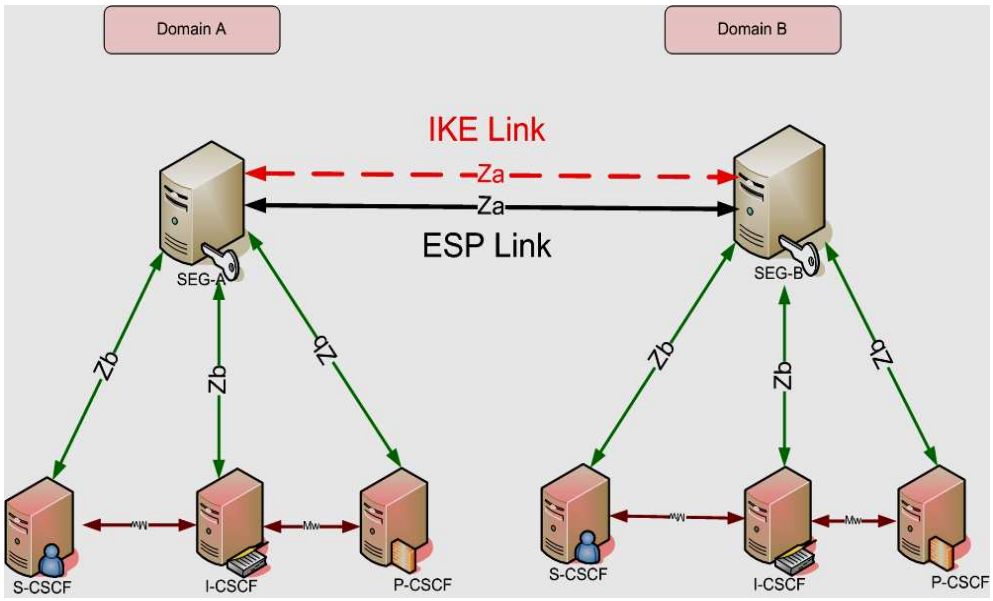

Figure 11 IMS Inter-Domain Gateways

7.2. IPSec Implementation Architecture

The IPSec implementation operates in SEG environment, affording protection to IP traffic. The protection is provided according to the requirements defined by Security Policy Database (SPD) that is established and maintained by a system administrator. In general, packets are selected for one of three processing modes based on IP and transport layer header information matched against entries in the database (SPD). A packet is either afforded IPSec security services, discarded, or allowed to bypass IPSec, based on applicable database policies identified by the selectors. IPSec provides security services at IP layer by enabling a system to select the required security protocols, determine the algorithms to be use for the service, and to provide the cryptographic keys required for the requested services. It can be used to protect one or more links between a pair of SEGs, or between a SEG and a host. The set of security services that IPSec can provide includes access control, data integrity protection, data origin authentication, anti-replay protection and limited traffic flow confidentiality. Because these services are provided at IP layer, they can be used by any higher layer protocol.

IPSec uses two protocols to provide traffic security i.e. Authentication Header (AH) and Encapsulating Security Payload (ESP). These protocols may be applied alone or in combination with each other to provide a desired set of security services in IPv4 and IPv6. Each protocol supports two modes of use i.e. transport mode and tunnel mode. In transport mode, the protocols provide protection primarily for upper layer protocols. Tunnel mode is typically used to tunnel IP traffic between two SEGs. The difference is that in transport mode IPSec offers limited protection to IP headers, whereas in tunnel mode full IP datagram is protected [28]. The components of IPSec security architecture are:

- Security Protocols - Authentication Header and Encapsulating Security Payload.

- Security Associations - definitions of Security Policy Database (SPD) and Security Association Database (SAD) as well as management and usage of security associations.
- Key Management - distribution of cryptographic keys use for security protocols (namely Internet Key Exchange (IKE).
- Algorithms used for encryption and authentication.

7.2.1 Security Associations

The concept of security association is germane to IPSec. A security association (SA) is set of policy and key(s) used to protect information and can be formally defined as the relationship between two SEGs that allows the protection of information communicated between them and that defines how they are going to use security services to secure their communications. It includes information on authentication and/or encryption algorithms, cryptographic keys and key lengths as well as initialization vectors (IV) that are shared between entities. A SA is unidirectional; so typically two SAs are needed for bidirectional flow of traffic—one for inbound (read) traffic and one for outbound (write) traffic. Security protocols make use of security associations (SAs) as they provide security services. This relationship includes a shared symmetric key and security attributes describing the relationship. It is uniquely identified by security parameter index (SPI) and destination IP address [20].

The management of SAs involves two databases i.e. SPD and SAD. The SPD contains policies by which all inbound and outbound traffic is categorized on host or security gateway. The SAD is a container for all active SAs, and related parameters. A set of selectors (IP layer and upper layer (e.g., TCP and UDP) protocol field values) is used by SPD to map traffic to specific SA. This relationship is represented by set of information that can be considered as a contract between the SEGs. The information must be agreed upon and shared between all the SEGs. All SEGs must adhere to the SA for secure communications to be possible. When accessing SA attributes, SEGs use a pointer or identifier referred to as Security Parameter Index (SPI) [25].

7.2.2. Encapsulating Security Payload

The security protocol used in NDS/IP for encryption, data integrity protection and authentication is IPSec Encapsulating Security Payload (ESP) [20] in tunnel mode i.e. full IP datagram, including IP header is encapsulated in the ESP packet. The ESP provides confidentiality, data origin authentication, data integrity protection, an anti-replay service, and limited traffic flow confidentiality. The set of services provided depends on options selected at the time of security association establishment and on the placement of implementation. The anti-replay service may be selected only if data origin authentication is selected, and its selection is solely at the discretion of the receiver.

For encryption, Triple DES (3DES) [18] algorithm is mandatory, while for data integrity and authentication both MD5 [21] and SHA-1 [22] can be used. The Encapsulating Security Payload (ESP) header is designed to provide a mix of security services in IPv4 and IPv6. The ESP header is inserted before an encapsulated IP header in tunnel mode. Thus the format of ESP packets for a given SA is fixed, for the duration of the SA. The ESP Header format is given in the figure 7. The tunnel mode ESP is employed by SEGs to protect transit traffic. The *inner* IP header carries ultimate source and destination addresses, while an *outer* IP header may contain distinct IP addresses usually addresses of security gateways. In tunnel mode, ESP protects the entire inner IP packet, including the entire inner IP header.

If authentication is selected, encryption is performed first, before the authentication, and the encryption does not encompass the Authentication Data field. This order of processing facilitates rapid detection and rejection of replayed or counterfeit packets by the receiver, prior to decrypting the packet, hence potentially reducing the impact of *denial of service attacks*. It also allows for the possibility of parallel processing of packets at the receiver, hence decryption can take place in parallel with authentication. Since Authentication Data is not protected by encryption, a keyed authentication algorithm must be employed to compute the Integrity Check Value (ICV). If authentication is selected for the SA, the sender computes ICV over ESP packet minus the Authentication Data [20]. Thus the SPI, Sequence Number, Payload Data, Padding (if present), Padding Length, and Next Header are all encompassed by ICV computation. Note that the last 4 fields will be in ciphertext form, since encryption is performed prior to authentication.

7.3 Internet Security Association and Key Management Protocol (ISAKMP)

Internet Security Association and Key Management Protocol (ISAKMP) [27] is used for negotiating, establishing, modification and deletion of security associations and related parameters. ISAKMP combines security concepts of authentication, key management, and security associations to establish the required security for government, commercial, and private communications on the Internet. The ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA). SAs contain all the information required for execution of various network security services, like IP layer services, header authentication, payload encapsulation, transport or application layer services and self-protection of negotiation traffic. The ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of key generation technique, encryption algorithm and authentication mechanism.

The ISAKMP is distinct from key exchange protocols in order to separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs. The ISAKMP is intended to support the negotiation of SAs for security protocols at all layers of network stack. By centralizing the management of the security associations, ISAKMP reduces the amount of duplicated functionality within each security protocol and can also reduce connection setup time, by negotiating a whole stack of services at once. The ISAKMP is a protocol which provides a framework for authentication and key exchange but does not define them. It is designed to be key exchange independent; that is, it is designed to support many different key exchanges. It supports Security Association (SA) and key management in an Internet environment. It also defines the procedures for the authentication of peers, creation and management of SAs, key generation techniques, and treatments for denial-of-service and reply attacks. SA establishment is a part of the key management protocol defined for IP based networks. SA supports different encryption algorithms, authentication mechanisms, and key establishment algorithms for other security protocols, as well as IP security.

When processing an outgoing IP packet for authentication, the first step is to locate the appropriate security association. All security associations are unidirectional. When accessing SA attributes, entities use an identifier referred as Security Parameter Index (SPI). The SPI is an identifier for SA relative to security protocols and each security protocol has its own SPI-space. In order to identify SA, the SPI is used together with Domain of Interpretation (DOI) which defines payload formats, exchange types,

naming conventions, security policies, and cryptographic algorithms and modes, and is used to interpret payloads of ISAKMP payloads. The selection of the appropriate SA for an outgoing IP packet is based at least upon sending user identity and destination address. When host-oriented keying is in use, everyone sending user identity will share the same SA to a given destination. When user-oriented keying is in use, then different users or possibly even different applications of same user might use different SAs. ISAKMP provides the protocol exchanges to establish a SA between negotiation server entities followed by the establishment of a SA by the negotiation server entities on behalf of some protocols such as AH/ESP [27].

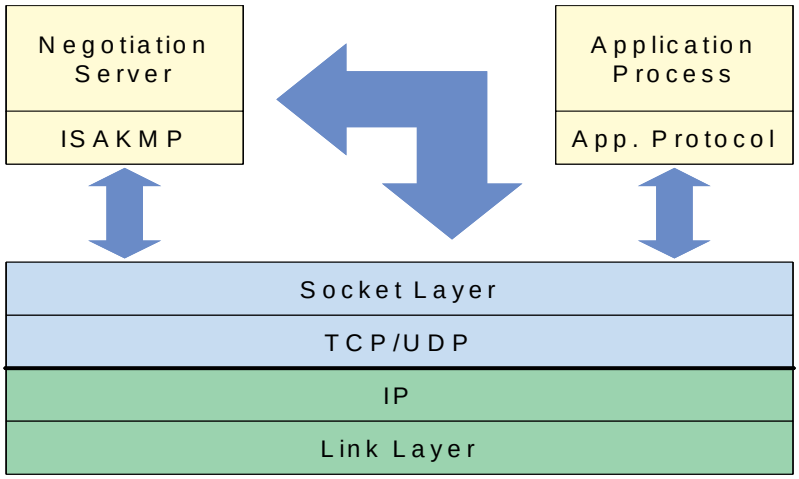

Figure 12: ISAKMP Relationships

For public key cryptography, key exchange function in ISAKMP includes key establishment method, authentication, symmetry, Perfect Forward Secrecy (PFS), and back traffic protection. ISAKMP users should choose additional key establishment algorithms based on their requirements. ISAKMP does not specify a specific key exchange and communication protocol with trusted third parties or certificate directory services. There is a proposal for using Oakley key exchange in conjunction with ISAKMP. To protect network from denial-of-service, ISAKMP uses anti-clogging-token cookie. ISAKMP also prevents connection hijacking by linking authentication, key exchange and SA exchanges. The ISAKMP provides protection against attacks, which include interception, insertion, deletion, modification of messages, reflecting messages, re-playing old messages and redirecting messages. The linking of the ISAKMP SA exchanges prevents the insertion of messages in the protocol exchange. The ISAKMP protocol state machine is defined so deleted messages will not cause a partial SA to be created, the state machine will clear all state and return to idle. The state machine also prevents reflection of a message from causing harm. The requirement for a new cookie with time variant material for each new SA establishment prevents attacks that involve replaying old messages. The ISAKMP authentication requirement prevents an SA from being established with other than the intended party. Messages may be redirected to a different destination or modified but this will be detected and SA will not be established.

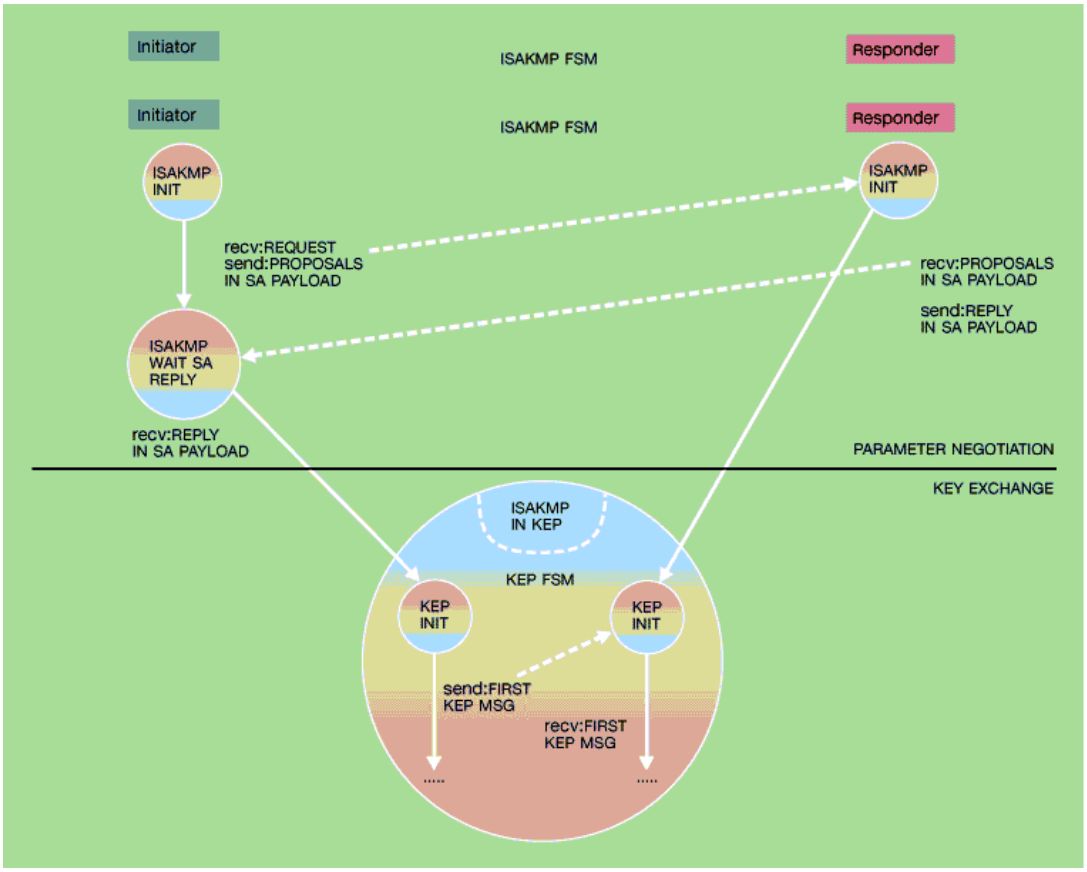

Figure 13: ISAKMP State Machine

The ISAKMP supports Internet Security DOI which supports naming and interpretation of security services. With DOI, users can design their own security environment such as security policies, cryptographic algorithms, and modes. It defines procedures and packet formats for peer authentication creation and management of SAs and techniques for key generation. It also includes mechanisms that mitigate certain threats e.g., denial-of-service (DOS) and anti-replay protection. The ISAKMP operates in two phases; in phase 1 the peers establish ISAKMP SA i.e. they authenticate and agree on the used mechanisms to secure further communications and in phase 2 ISAKMP SA is used to negotiate further protocol SAs e.g., IPSec/ESP SA. After the initial establishment of ISAKMP SA, multiple protocol SAs can be established [28].

7.4 Internet Key Exchange (IKE)

The Internet Key Exchange (IKE) [26] automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual pre-configuration. Specifically, IKE provides these benefits:

- Eliminates the need to manually specify all IPSec security parameters in crypto maps at both peers.
- Allows specifying a lifetime for IPSec security association.

- Allows encryption keys to change during IPSec sessions.
- Allows IPSec to provide anti-replay services.
- Permits Certification Authority (CA) support for manageable, scalable IPSec implementation.
- Allows dynamic authentication of peers.

7.4.1 IKE Operation

The Oakley and ISAKMP define a method to establish an authenticated key exchange which includes payloads construction, information payloads carry, the order in which they are processed and how they are used. While Oakley defines *modes*, ISAKMP defines *phases*. The relationship between two is straightforward and IKE presents different exchanges as modes which operate in one of two phases. Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate and is called the ISAKMP Security Association (SA). The *Main Mode* and *Aggressive Mode* each accomplish a phase 1 exchange and must only be used in phase 1. Phase 2 is where SAs are negotiated on behalf of services such as IPSec or any other service which needs key material and/or parameter negotiation. The *Quick Mode* accomplishes phase 2 exchange and must only be used in phase 2. The *New Group Mode* is not really phase 1 or phase 2. It follows phase 1, but serves to establish new group which can be used in future negotiations.

The ISAKMP SA is bi-directional i.e. once established; either party may initiate Quick Mode, Informational, and New Group Mode Exchanges. With the use of ISAKMP phases, an implementation can accomplish very fast keying when necessary. A single phase 1 negotiation may be used for more than one phase 2 negotiation. Additionally a single phase 2 negotiation can request multiple SAs. With these optimizations, an implementation can see less than one round trip per SA as well as less than one DH exponentiation per SA. The *Main Mode* for phase 1 provides identity protection. When identity protection is not needed, *Aggressive Mode* can be used to reduce round trips even further. This protocol does not define its own DOI. The ISAKMP SA, established in phase 1, may use the DOI and situation from a non-ISAKMP service. In this case an implementation may choose to restrict use of the ISAKMP SA for establishment of SAs for services of the same DOI. Alternately, an ISAKMP SA may be established with zero value in both DOI and in this case implementations will be free to establish security services for any defined DOI using this ISAKMP SA. The IKE implementations should support 3DES for encryption, the Digital Signature Standard, RSA signatures and authentication with RSA public key encryption.

7.4.2 IKE Exchanges

There are two basic methods used to establish authenticated key exchange i.e. *Main Mode* and *Aggressive Mode*. Each mode generates authenticated keying material from an ephemeral Diffie-Hellman exchange. *Main Mode* must be implemented but *Aggressive Mode* should be implemented. In addition, *Quick Mode* must be implemented as mechanism to generate fresh keying material and negotiate non-ISAKMP security services and *New Group Mode* should be implemented as a mechanism to define private groups for Diffie-Hellman exchanges. Exchanges conform to standard ISAKMP payload syntax, attribute encoding, timeouts and retransmits of messages, and informational messages. The SA payload must precede all other payloads in phase 1 exchange. The Diffie-Hellman public value passed in a KE payload, in either phase 1 or phase 2 exchanges must be the length of the negotiated Diffie-Hellman group enforced, if necessary, by pre-pending the value with zeros. The length of nonce payload must be between 8 and 256 bytes inclusive [28].

The exchanges in IKE are not opening ended and have fixed number of messages. Receipt of a Certificate Request payload must not extend the number of messages transmitted or expected. The SA negotiation is limited with *Aggressive Mode*. Due to message construction requirements the group in which the Diffie-Hellman exchange is performed cannot be negotiated. In addition, different authentication methods may further constrain attribute negotiation. For example, authentication with public key encryption cannot be negotiated and when using the revised method of public key encryption for authentication the cipher and hash cannot be negotiated. For situations where the rich attribute negotiation capabilities of IKE are required *Main Mode* may be required. During security association negotiation, initiator present offers for potential security associations to responders. Responders must not modify attributes of any offer, attribute encoding excepted. If the initiator of an exchange notices that attribute values have changed or attributes have been added or deleted from an offer made, that response must be rejected.

7.5 Public Key Infrastructure (PKI)

Public key cryptography, also referred to as asymmetric cryptography, utilizes a pair of keys, one private and other public which are mathematically related. Information is encrypted with the public key, and can only be decrypted with corresponding private key. In PKI, public keys of all users are published in an open directory, facilitating communications between all parties. The private key is not shared, only the public key is made public. Public key cryptography can also be used to create and verify digital signatures which are appended with messages to provide proof of authentication, integrity and non-repudiation. PKI Forum's "PKI basics - A Technical Perspective" [29] provides a concise vendor neutral introduction to the PKI technology, addressing the following issues:

- Security policies that define rules under which cryptographic systems should operate.
- Procedures to generate store and manage keys.
- Procedures how keys and certificates are generated, distributed and used.

A Public Key Infrastructure is a combination of policies and procedures, hardware and software. PKI is based on digital IDs known as ‘digital certificates’ that bind the user’s digital signature to his or her public key. A PKI should consist of the following components.

- A Security Policy
- Certification Authority (CA)

A security policy sets out and defines top-level direction on information security, as well as processes and principles for the use of cryptography. Typically it will include statements on how to handle keys and valuable information, and will set the level of control required to match the levels of risk. The CA system is the trust basis of PKI, since it manages public key certificates for their whole life cycle. The CA performs the following tasks:

- Issue certificates by binding identity of a user or SEG to a public key with a digital signature.
- Schedule expiry dates for certificates.
- Ensure certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs).

The PKI must ensure that the CA’s private key is held in a tamper-resistant security module, and provision must be made for back-up copies for disaster recovery purposes. Access to the CA and RA should be tightly controlled. All certificate requests should be digitally signed to detect and prevent

hackers from deliberately generating counterfeit certificates. All significant events performed by the CA/RA system should be recorded in a secure audit trail, where each entry is time/date stamped and signed to ensure that entries cannot be falsified.

The cross-certification is a process that establishes a trust relationship between two authorities. When Certification Authority A is cross-certified with Certification Authority B, this implies that A has chosen to trust certificates issued by B. The cross-certification process enables the users under both authorities to trust the other authority's certificates. Trust in this context equals being able to authenticate. There are two types of cross-certification processes:

7.5.1 Manual Cross-certification

In manual cross-certification, mutual cross-certifications are established directly between Certification Authorities. The authority makes decisions about trust locally. When Certification Authority A chooses to trust Certification Authority B, then authority A signs the certificate of authority B and distributes the new certificate (B's certificate signed by A) locally. The disadvantage of this approach is that it often results in scenarios where there is need to large number of certificates available for entities doing the trust decisions. However, all the certificates can be configured locally and are locally signed, so their management is often flexible.

7.5.2 Bridge Cross-certification

The Bridge CA is a concept that reduces the number of certificates that need to be configured for entity that does certificate checking. The name "bridge" is descriptive; when two authorities are mutually cross-certified with bridge, the authorities do not need to know about each other. Authorities can still trust each other because trust in this model is transitive (A trusts bridge, bridge trusts B, thus A trusts B and vice versa).

The bridge CA acts like a bridge between the authorities. However, two authorities shall also trust that bridge does the right thing for them. All the decisions about trust can be delegated to the bridge, which is desirable in some use cases. If the bridge decides to cross-certify with an authority M, the previously cross-certified authorities start to trust M automatically. Bridge CA style cross-certifications are useful in scenarios where all entities communicate a common Trusted Third Party. If an authority needs to restrict the trust or access control derived from Bridge CA, it additionally needs to implement those restrictions.

7.6 PKI architecture for NDS/AF (Network Domain Security/Authentication Framework)

This section defines PKI architecture of NDS/AF (Network Domain Security/Authentication Framework). The architecture uses a simple access control method, i.e. every element which is authenticated is also providing a service. The architecture does not rely on bridge CAs, but instead uses direct cross-certifications between security domains. This enables easy policy configurations in the SEGs. Each security domain has at least one Local Certificate Authority (LCA) and one Domain Certificate Authority (DCA) dedicated to it. The LCA of the domain issues certificates to SEGs in the domain that have interconnection with SEGs in other domains. The DCA of the domain issues certificates to LCAs of other domains with which operator’s SEGs have interconnection. This specification describes profile for various certificates and method for creating cross-certificates. All the certificates are based on Internet X.509 certificate profile [29].

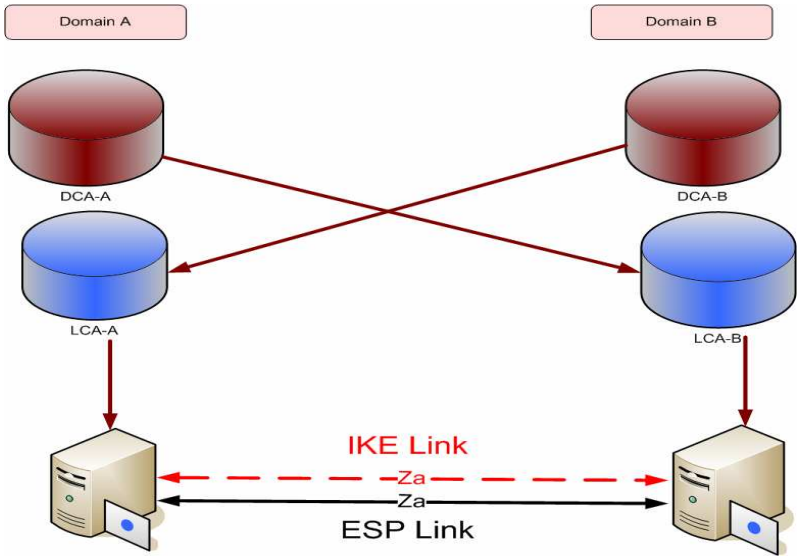

Figure 14 Inter-Domains Certificate Distribution

The LCA issues certificates for SEGs that implement Za interface. When SEG of security domain A establishes a secure connection with SEG of domain B, they are able to authenticate each other. The mutual authentication is checked using the certificates LCAs issued for the SEGs. When a roaming agreement is established between domains, the DCA cross-certify LCA of peer operator. The created cross-certificates need only to be configured locally to each domain. The cross-certificate, which DCA-A of security domain A created for LCA of security domain B, shall be available for domain A SEG which provides Za interface towards domain B. Equally the corresponding certificate, which DCA-B of security domain B created for LCA of security domain A, shall be available for domain B SEG which provides Za interface towards domain A.

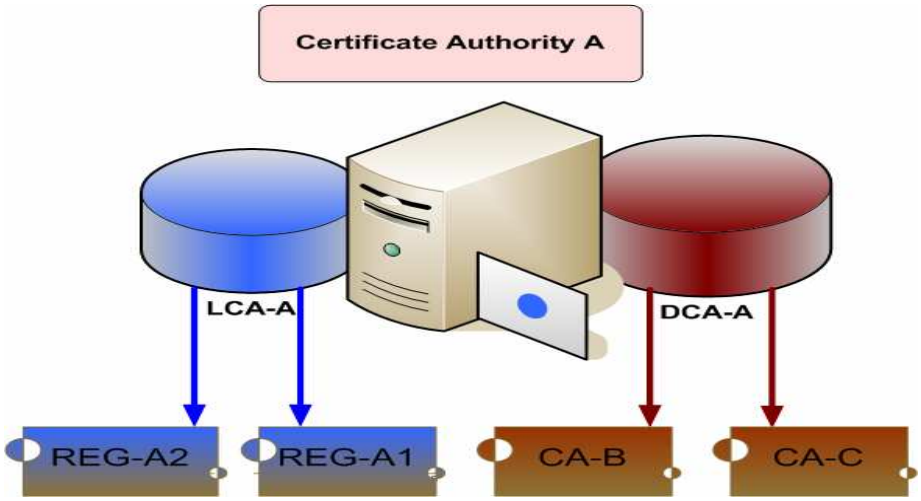

Figure 15 Certificate Hierarchy of CA-A

The public key of DCA is stored securely in each SEG within operator's domain. This allows SEG to verify cross certificates issued by its operator's DCA. It is assumed that each operator domain could include 2 to 10 SEGs. An operator may decide to set up both LCA and DCA as a single CA, i.e. separation of CAs is not required. The NDS/AF is initially based on a simple trust model that avoids introduction of transitive trust and/or additional authorisation information. The simple trust model implies manual cross-certification [25].

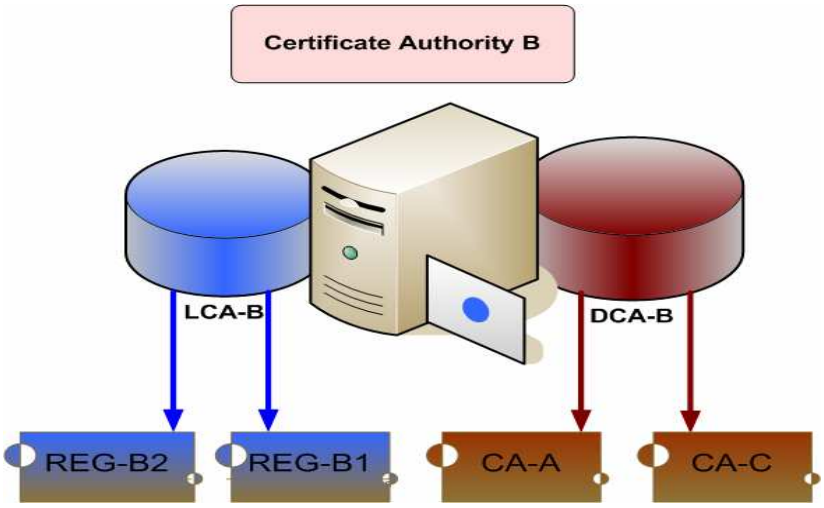

Figure 16 Certificate Hierarchy of CA-A

The creation of a roaming agreement only involves use of private keys of DCAs. There is no need for the operators to use private keys of their respective LCAs in forming a roaming (or interconnection) agreement. When creating new cross-certificate, the DCA should use basic constraint extension and set path length to zero. This inhibits the new cross-certificate to be used in signing new CA certificates. The validity of certificate should be set sufficiently long. The cross-certification process needs to be done again when the validity of cross-certificate is ending. When the new cross-certificate is available to SEG, all that needs to be configured in SEG is the DNS name or IP address of the peering SEG gateway. The authentication can be done based on the created cross-certificates.

8. Security Management for HTTP-Based Services

The Ut interface is reference point between the User and Application Server (AS) that enables users to securely manage and configure their network services-related information hosted on an AS. Users can use Ut reference point to create public service identities, such as a resource list, and manage authorization policies that are used by the service. Examples of services that utilize the Ut reference point are presence and conferencing. The AS may need to provide security for the Ut reference point. HTTP is chosen data protocol for the Ut reference point that performs the functionality to manage data traffic for HTTP based applications. Thus securing the Ut interface means to achieve confidentiality and data integrity protection of HTTP-based traffic.

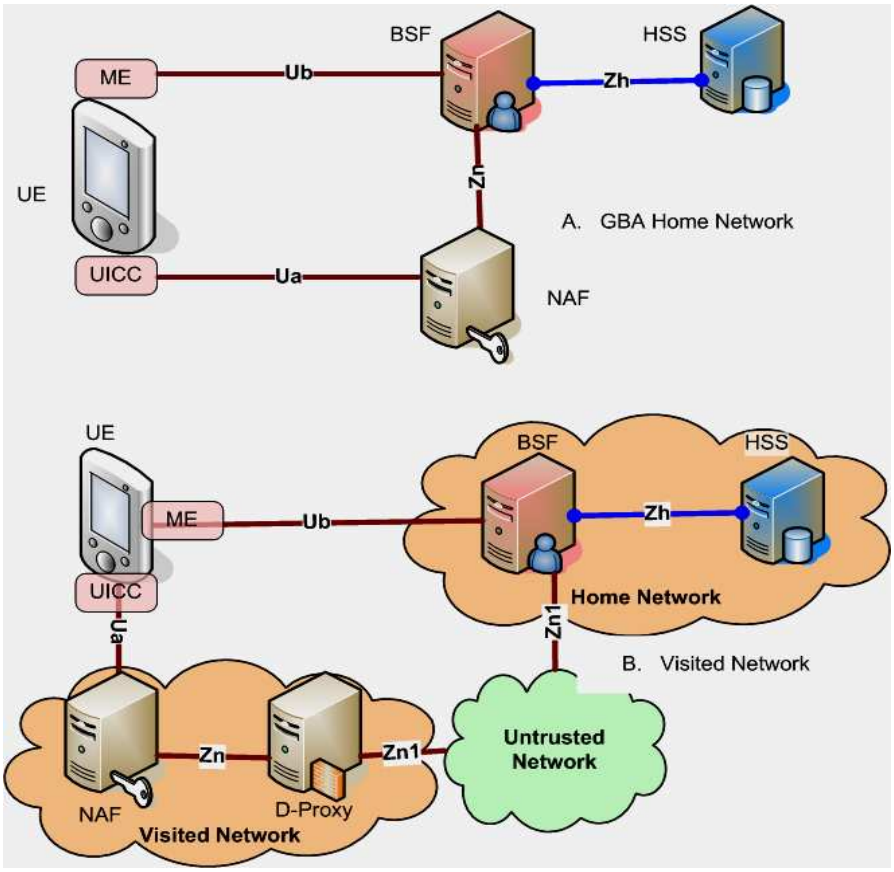

Figure 17 GBA Architecture

The authentication and key agreement for Ut interface is also based on AKA. The IMS defines Generic Bootstrapping Architecture (GBA) [12] as a part of Generic Authentication Architecture (GAA) that performs mutual authentication between Bootstrapping Server Functions (BSF) and the UE. AKA generates session keys and enable further applications provided by the Network Application Function (NAF) that issues subscriber certificates using an applications protocol secured by bootstrapped session keys. The authentication in Ut interface is performed by authentication proxy. In terms of GBA, the authentication proxy is another type of NAF. Traffic in Ut interface goes through authentication proxy and is secured using the bootstrapped session key.

The Ut interface employs Transport Layer Security (TLS) [11] for both confidentiality and integrity protection. It utilized generic bootstrapping architecture to assure the application servers (ASs) that the request is coming from an authorized subscriber of mobile network operator. When HTTPS request is sent to AS through AP, AP performs UE authentication. The AP may insert the user identity when it forwards the request to application server. Figure 18 presents the architectural view of using AP for different IMS SIP services e.g. presence, messaging, conferencing etc.

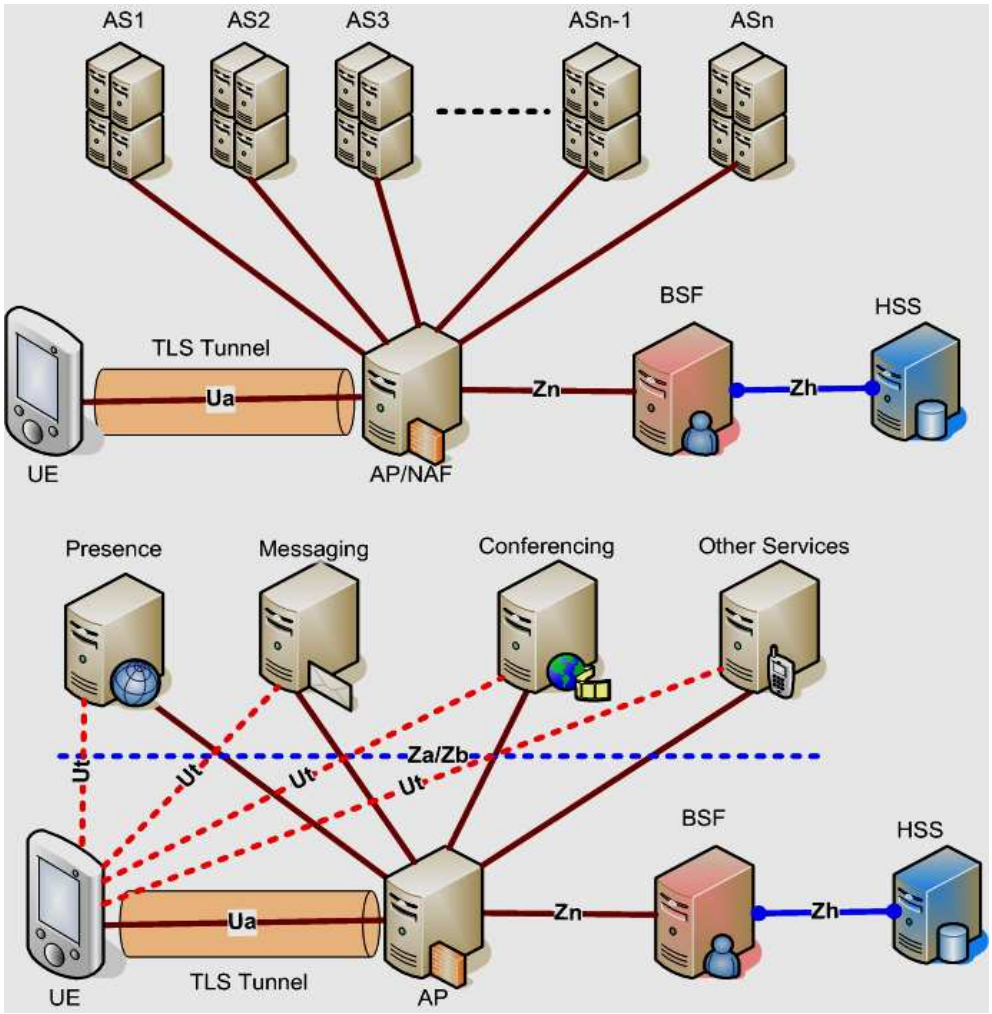

Figure 18*:* Authentication Proxy

The UE shall manipulate own data such as groups, through Ua/Ut reference point [9]. The reference point Ut will be applicable to data manipulation of IMS based SIP services, such as Presence, Messaging and Conferencing services. When HTTPS client starts communication via Ua reference point with NAF, it shall establish a TLS tunnel with NAF. The NAF is authenticated to HTTPS client by means of a public key certificate. The HTTPS client will verify that the server certificate corresponds to FQDN (Fully Qualified Domain Name) of AP it established the tunnel with.

Now we briefly explain the procedure as: HTTPS client sends HTTP request to NAF inside TLS tunnel. In response to HTTP request over Ua interface, AP will invoke HTTP digest with HTTPs client in order to perform client authentication using the shared keys. On the receipt of HTTPS digest from AP, client will verify that FDQN corresponds to the AP that established the TLS connection with, if not the client will terminate TLS connection with the AP. In this way UE and AP are mutually authenticated as the TLS tunnel endpoints.

Here is an example that explains how application residing on UICC (Universal Integrated Circuit Card) may use TLS over HTTP in Generic Authentication Architecture (GAA) mechanism to secure its communication with Authentication Proxy (AP). The GBA security association between a

UICC-based application and AP can be established as: The ME (Mobile Equipment) executes the bootstrapping procedure with the BSF supporting the Ub reference point. The UICC, which hosts the HTTPS client, runs the bootstrapping usage procedure with AP supporting the Ua reference point [13].

9. Fokus Open IMS Testbed

In face of current challenges within telecommunications market are mainly a consequence of insufficient early access to new enabling technologies by all market players, the Fraunhofer Institute Fokus, known as a leading research institute in the field of open communication systems, has established within support of German Ministry of Education and Research (BMBF) a 3G beyond Testbed, known as "National Host for 3Gb Applications" [30]. This Testbed provides technologies and related know-how in the field of fixed and wireless next generation network technologies and related service delivery platforms.

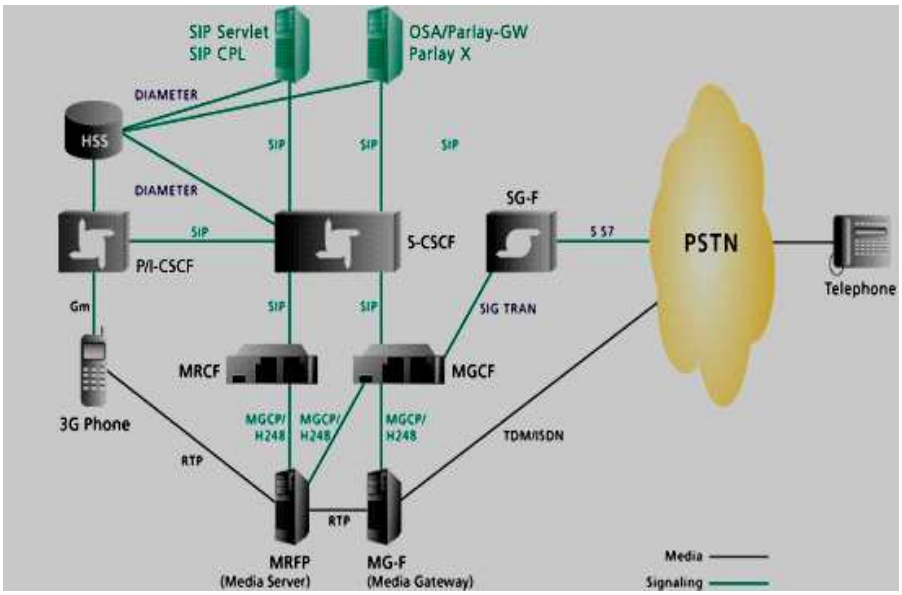

Figure 16 Fokus Fraunhofer IMS Testbed

As such the testbed is quite complex by its nature, FOKUS has established within this an "Open IMS Playground @ FOKUS" [31] based on different access technologies, infrastructure components and management tools. FOKUS implemented all core components of IMS and enriched this base infrastructure with components from commercial vendors. Particularly Service Delivery Platform (SDP) diversity, promoted within IMS, is supported by providing different service platforms, such as Open Service Access (OSA) /Parlay, JAIN Service Logic Execution Environments (SLEE), Web Services / Parlay X, SIP Servlets, Call Processing Language (CPL) etc on top of multiplicity of access technologies including an exclusive 3G UMTS cell [32].

The FOKUS Open IMS Playground is deployed as an open technology test field with target to validate existing and emerging IMS standards and to extend the IMS appropriately to be used on top of new access networks as well as to provide new seamless multimedia applications. All major IMS core components, i.e., x-CSCF, HSS, MG, MRF, Application Servers, Application Server Simulators, service creation toolkits, and demo applications are integrated into one single environment and can be

used and extended for R&D activities by academic and industrial partners. All these components can be used locally on top of all available access technologies or can be used over a IP tunnels remotely.

9.1 Description of IMS Testbed

Here we will discuss high level description of FOKUS 3Gbeyond/NGN Testbed and positioning of IMS playground within the testbed architecture. In principle the testbed comprises three layers:

1) The lowest level is called the network plane. With the introduction of 3G networks it became clear that these networks have to integrated with other wireless and fixed access networks, such ISDN, GSM, WLAN, WiMAX, digital video broadcasting, satellite, Internet, etc. including the related end systems to provide seamless services for converging networks.

2) On top of network, there is seamless service control and management layer, constituted signalling and management components and valued added service provisioning components forming the Service Delivery Platforms.

3) The application plane makes use of underlying service layer for the provision of advanced seamless multimedia applications. It provides a basis for the validation of underlying entities. Sophisticated application development tools and model driven architecture (MDA) tools provide a highly comfortable way to develop services.

Across all these planes FOKUS provides engineering, conformance testing, measurement, and management tools. Thus FOKUS provides for all layers more than one realization option, which results in plenty of combinations and a high complexity of such a testbed. However, there is need for performing feasible R&D projects in the context of NGN. In addition, the infrastructure is provided to third parties on an "as needed" basis. Knowing about this overall complexity, FOKUS has decided to provide technology focal points within the 3Gb testbed. Particularly the area of SDPs is considered key for seamless multimedia service provision. Therefore, FOKUS has created in 2003 the first open OSA/Parlay Playground. Based on the success of this testbed and its global recognition, FOKUS has opened in mid 2004 the Open IMS playground.

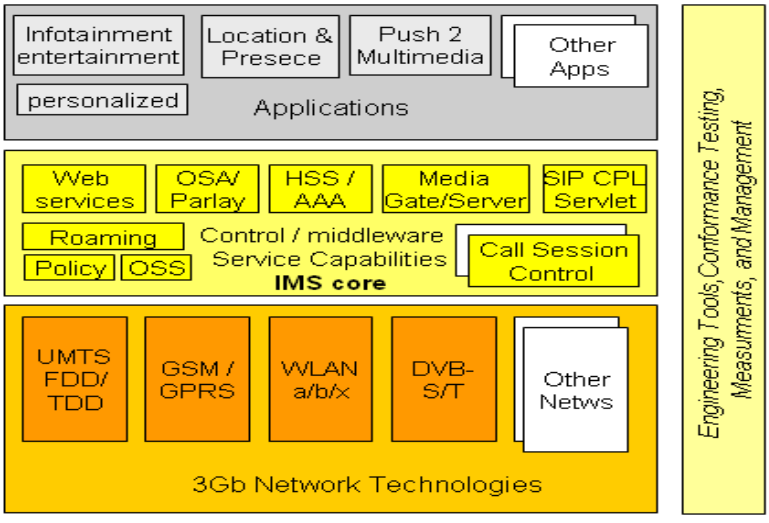

Figure 17 Descriptions of FOKUS Open IMS within 3Gb Testbed

In order to place the IMS playground within the aforementioned 3Gb testbed, we have IMS mainly within the service control and management layer, since it is an overlay service provisioning platform (see figure 17). We can recognise so-called Call State Control Functions (CSCF), forming the unified signalling core of the IMS on top of the underlying transport networks controlled via policies. Media Gateways and Media Server support potentially require adaptation of multimedia information for specific QoS requirements. However, the main part of IMS constitutes of subscription system, realizes with the Home Subscriber Servers (HSS) providing Authentication, Authorisation functions, as well as many different application server options, ranging from OSA/Parlay to SIP application server supporting Web Services, SIP Servlets, SIP CPL, etc.

The signalling within the IP Multimedia subsystem bases on the Session Initiation Protocol (SIP). The "Open IMS playground" uses the SIP Express Router [33], which is recognised worldwide as SIP reference implementation, to perform all call session control functionality. The SIP Express Platform offers a configurable, extendible as well as reliable SIP-based service provisioning infrastructure. Besides its rich base of functionalities the SIP Express platform allows providers and users to extend their service offerings through different interfaces:

- Plug & Play interfaces allow providers to extend the functionalities of the SER platform by defining new modules and integrating them with the SIP Express platform.
- The application server interface allows providers to build new services by combining the features of the platform into novel services. In the context of IMS this is the appropriate way for provisioning a 3GPP compliant Virtual Private Network.
- The SIP Express Configuration Language allows the operators to customize the behaviour of the platform to accommodate specific operation requirements and environments.
- The End-User interface of the SIP Express platform provides the end users with web and CPL based methods for defining and customizing their own services.
- Within the Open IMS the SIP Express Router (SER) is extended and used as x-CSCF and as an Application Server core.

10. Conclusions and Future Work

The proposed security framework will be used to provide secure and protected platform for testing and validating different protocols and services for IMS and NGN at Fokus IMS Testbed. In this article we have presented the architecture and development of IMS security framework which is in align with technical specification of 3GPP. This research work is done for developing the secure IMS architecture and Secure Service Provisioning [34] Framework. The important features of this framework including user and network authentication in a secure fashion, providing inter and intra domains security for roaming and multi domains communication, and security management for SIP based application as well as HTTP based services to establish a secure and protected environment based platform for IMS playground within 3Gb (3rd Generation and beyond) Testbed at Fokus, Fraunhofer. The design utilizes inter-domains security gateways for generating and managing keys and certificates for secure and confidential communication for roaming users.

In future work we are working to design and develop Intrusion Detection and Prevention (IDP) System for IP Multimedia System (IMS) and Next Generation All IP Networks to monitor, detect and prevent the security attacks and threats to provide secure and protected environment to IMS operators. As we know that for IMS, most of the security work like authentication, encryption, confidentiality

and reliability are standardized by 3GPP [2] releases 5 and onwards that provides security at first level. But if an intruder penetrates into the network through security trapdoors by breaking first level security or misuse network resources and services, than there should be check to monitor, detect and stop activities of these hackers and intruders which are harmful not only to steel users confidential information but also dangerous for network operators to break and damage the network operators resources and assets. This IDP will provide measures for monitoring, detecting and preventing such type of malicious activities.

References

[1] Third Generation Partnership Project Technical Specification Group Services and System Aspects, IP Multimedia Subsystems (IMS), 3GPP TS 23.228 V6.7.0 (2004-09).
[2] Third Generation Partnership Project (3GPP). www.3gpp.org.
[3] Third Generation Partnership Project 2 (3GPP2). www.3gpp2.org.
[4] ETSI TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) WG. http://portal.etsi.org/tispan/
[5] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, “SIP: Session Initiation Protocol”, IETF RFC 3261 (June 2002).
[6] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, “Diameter Base Protocol”, IETF RFC 3588 (Sep. 2003).
[7] M. Poikselkae,G. Mayer, H. Khartabil, A. Niemi, “The IMS, IP Multimedia Concepts and Services in the Mobile Domain”ISBN 0-470-87133-X, John Willey & Sons Ltd. West Sussex, England, 2004.
[8] M. Sher, T. Magedanz: "Security Associations Management (SAM) Model for IP Multimedia System (IMS)", NetCon05, Network Control and Engineering for QoS, Security and Mobility, IFIP TC6 Conference, sponsored by WG6.2 (Network and Internet work Architectures), WG6.6 (Management of Networks and Distributed Systems), WG6.7 (Smart Networks) and WG6.8 (Mobile and Wireless Comm.), Lannion, France, November 14-18, 2005.
[9] S. Bellovin, J. Ioannidis, A. Keromytis, R. Stewart, “On the Use of Stream Control Transmission Protocol (SCTP) with IPSec”, IETF, RFC 3554 (July 2003).
[10] Third Generation Partnership Project Technical Specification Group Services and System Aspects, Network Domain Security (NDS); IP Network Layer Security, TS 33.310 V6 (2004).
[11] Third Generation Partnership Project Technical Specification Group Services and System Aspects, “Access to Network Application Functions using HTTP over TLS (HTTPS)”, 3GPP TS 33.222 V6.1.0 (2004-09).
[12] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) (Release 7), 3GPP TS 33.220 V7 (2005).
[13] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Access to Network Application Functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (Release 7), 3GPP TS 33.222 V7 (2005).
[14] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 6); 3GPP, TS 33.102 V6 (2004).
[15] M. Sher, T. Magedanz: "Network Access Security Management (NASM) Model for Next Generation Mobile Telecommunication Networks", IEEE/IFIP MATA’2005, 2nd International Workshop on Mobility Aware Technologies and Applications - Service Delivery Platforms for Next Generation Networks, Montreal, Canada, October 17-19, 2005, Proceeding Springer-Verlag, Berlin Heidelberg LNCS 3744-0263, ISSN: 0302-9743, (pp. 263-272), 2005.
[16] Third Generation Partnership Project Technical Specification Group Services and System Aspects, 3G Security; “Access Security for IP-based services (Release 6)”, 3GPP, TS 33.203 V6.4.0 (2004-09).

[17] A. Niemi, J. Arkko, V. Torvinen, "HTTP Digest Authentication Using AKA", IETF RFC 3310 (2002).
[18] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, (Nov 1998).
[19] J. Arkko, V. Torvinen, G. Camarillo, A. Niemi, T. Haukka, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)", IETF RFC 3329 (2003).
[20] S. Kent, R. Atkinson "IPSec Encapsulating Security Payload, ESP, IPSec ESP", IETF RFC 2406 (1998).
[21] C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH", IETF RFC 2403 (1998).
[22] C. Madson, R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", IETF RFC 2404 (1998).
[23] R. Pereira, R. Adams, "The ESP CBC-Mode Cipher Algorithms" IETF RFC 2451 (1998).
[24] S. Frankel, R. Glenn, S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPSec" IETF RFC 3602 (2003).
[25] Third Generation Partnership Project Technical Specification Group Services and System Aspects, "Network Domain Security (NDS); IP Network Layer Security", 3GPP, TS 33.310 V6.5.0 (2004-06).
[26] D. Harkins, D. Carrel, "IKE: Internet Key Exchange", IETF RFC 2409 (1998).
[27] D. Maughan, M. Schertler, M. Schneider, J. Turner, "ISAKMP: Internet Security Associations and Key Management Protocol", IETF RFC 2408 (1998).
[28] M. Sher, T. Magedanz, W.T. Walter, "Inter-Domains Security Management (IDSM) Model for IP Multimedia Subsystem (IMS)", IEEE 1st International Conference on Availability, Reliability and Security (ARES 2006), and "International Symposium on Frontiers in Availability, Reliability and Security (FARES)", Vienna, Austria, 20th-22nd April 2006. http://www.ares-conf.org.
[29] William Stallings, "Cryptography and Network Security", Prentice Hall, New Jersey, 1998.
[30] Third Generation & Beyond (3Gb) Testbed, www.fokus.fraunhofer.de/national_host.
[31] IP Multimedia System (IMS) Playground www.fokus.fraunhofer.de/ims.
[32] T. Magedanz, K. Knüttel, D. Witszek: "The IMS Playground @ Fokus – an Open Testbed for Next Generation Network Multimedia Services", 1st Int. IFIP Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (Tridentcom), Trento, Italian, February 23 - 25, 2005, Proceedings pp. 2 – 11, IBSN 0-7695-2219-x, IEEE Computer Society Press, Los Alamitos, California.
[33] SIP Express Router (SER), www.iptel.org.
[34] M. Sher, T. Magedanz, "Secure Service Provisioning Framework (SSPF) for IP Multimedia System and Next Generation Mobile Networks" IWWST'05, 3rd International Workshop in Wireless Security Technologies, London, U.K. April 2005, IWWST'05 Proceeding, ISSN 1746-904X, pp. 101-106. http://www.iwwst.org.uk.