Secure Access to IP Multimedia Services Using Generic Bootstrapping Architecture (GBA) for 3G & Beyond Mobile Networks

Muhammad Sher
TU Berlin / Fokus Fraunhofer
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany
sher@fokus.fraunhofer.de

Thomas Magedanz
TU Berlin / Fokus Fraunhofer
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany
magedanz@fokus.fraunhofer.de

ABSTRACT

The IP Multimedia Subsystem (IMS) defined by Third Generation Partnership Projects (3GPP and 3GPP2) is a technology designed to provide robust multimedia services across roaming boundaries and over diverse access technologies with promising features like quality-of-service (QoS), reliability and security. The IMS defines an overlay service architecture that merges the paradigms and technologies of the Internet with the cellular and fixed telecommunication worlds. Its architecture enables the efficient provision of an open set of potentially highly integrated multimedia services, combining web browsing, email, instant messaging, presence, VoIP, video conferencing, application sharing, telephony, unified messaging, multimedia content delivery, etc. on top of possibly different network technologies. As such IMS enables various business models for providing seamless business and consumer multimedia applications. In this communication converged world, the challenging issues are security, quality of service (QoS) and management & administration. In this paper our focus is to manage secure access to multimedia services and applications based on SIP and HTTP on top of IP Multimedia Subsystem (IMS). These services include presence, video conferencing, messaging, video broadcasting, and push to talk etc. We will utilize Generic Bootstrapping Architecture (GBA) model to authenticate multimedia applications before accessing these multimedia services offered by IMS operators. We will make enhancement in GBA model to access these services securely by introducing Authentication Proxy (AP) which is responsible to implement Transport Layer Security (TLS) for HTTP and SIP communication. This research work is part of Secure Service Provisioning (SSP) Framework for IP Multimedia System at Fokus Fraunhofer IMS 3Gb Testbed.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]: C.2.0 General - *Security and protection*; C.2.1 Network Architecture and Design; C.2.3 Network Operation.

Q2SWinet'06, October 2, 2006, Torremolinos, Malaga, Spain.
Copyright 2006 ACM 1-59593-486-3/06/0010...$5.00.

General Terms

Algorithms, Management, Design, Reliability, Experimentation, Security, Standardization, Verification.

Keywords

IP Multimedia System, Generic Bootstrapping Architecture, Generic Authentication Architecture, Security and Privacy, Transport Layer Security, Authentication Proxy.

1. INTRODUCTION

With the emergence of mobile multimedia services, such as unified messaging, click to dial, across network multiparty conferencing and seamless multimedia streaming services, the convergence of networks (i.e. fixed–mobile convergence and voice–data integration) has started, leading to an overall Internet–Telecommunications convergence. In prospect of these 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 (Voice over Internet Protocol) and videoconferencing on top of globally emerging 3G (Third Generation) broadband packet networks. The IP Multimedia System (IMS) which is standardized by Third Generation Partnership Project (3GPP & 3GGP2) in releases 5 is an overlay network on top of GPRS/UMTS (General Packet Radio Systems/Universal Mobile Telecommunication Systems) networks and extended by ETSI TISPAN [2] for fixed line access network within the Next Generation Network (NGN) architecture.

The IMS provides all IP Service Delivery Platform (SDP) for mobile multimedia services provisioning e.g. VoIP, Video-telephony, Multimedia conferencing, Mobile Content, Push-to-Talk etc. and it is based on IETF protocols like SIP for session control, Diameter for AAA (Authentication, Authorization, and Auditing) and SDP (Service Delivery Protocol), RTP etc. Different components and parts of IMS are highlighted in figure 1 consisting IMS Core (P-CSCF, I-CSCF, S-CSCF), IMS Client (UE) and Application & Media Servers along with the concept of home network and visited network for roaming users on top of different access networks technologies.

The security and data privacy is a big challenge when there is integration of different networks and technologies. The integration of different access technologies causes much vulnerability and hackers get access to steal financial and confidential information. As these hackers networks are often beyond the law enforcement agencies of the today's communication world. So the question arises how to prevent these hackers for performing such attacks on the corporate networks. In order to provide confidentiality, security and privacy, the 3G authentication infrastructure is a valuable and milestone development and asset for 3G operators. This infrastructure consists of authentication centre (AuC), the USIM (Universal Subscriber Identity Module) or ISIM (IP Multimedia Services Identity Module) and AKA (Authentication and Key Agreement) Procedure.

It has recognized that this infrastructure could utilize to enable application function in the network and on the user side to enable shared keys. Therefore, Third Generation Partnership Project (3GPP) has provided the *bootstrapping of application security* to authenticate the subscriber by defining a Generic Bootstrapping Architecture (GBA) [3] based on Authentication and Key Agreement (AKA) protocol. The GBA model can be utilized to authenticate subscriber before accessing multimedia services and applications over HTTP. The candidate applications to use this bootstrapping mechanism include but are not restricted to subscriber certificate distribution. These certificates supports services including presence, conferencing, messaging and push to talk etc. provided by mobile operators. The GBA model has enhanced by implementing Generic Authentication Architecture (GAA) [4] to provide secure assess over HTTP using TLS (Transport Layer Security).

In prospective of the advancement of telecommunication, the Fraunhofer Fokus established a Third Generation & beyond (3Gb) Testbed and IMS Testbed [5] for research & development and educational purpose to provide state-of-the-art knowledge to engineers, researchers, educationists and technologists in this area of modern telecommunication. Fokus Fraunhofer has developed a Secure Service Provisioning (SSP) Framework [6] for IMS Testbed to provide security, privacy and authentication of subscriber as well as confidential and protection to the network resources of 3G operators.

The paper is organised as: section 2 is about IMS as platform for multimedia services, sections 3, 4 and 5 explain generic bootstrapping architecture, bootstrapping authentication procedure and its application usage procedure respectively. Section 6 discusses the use of authentication proxy for implementing TLS for securing multimedia services. In section 7, we will discus briefly the IMS Testbed at Fokus and than concludes the paper in last section.

2. IMS – Platform for Next Generation Multimedia Services

The IMS defines service provision architecture, and it can be considered as the next generation service delivery platform. It consists of modular design with open interfaces and enables the flexibility for providing multimedia services over IP technology. The IMS does not standardize specific services but uses standard service enablers e.g. presence, GLMS/XDMS etc. and supports inherently multimedia over IP, VoIP, Internet Multimedia and presence. In IMS architecture, SIP protocol use as the standard signaling protocol that establishes controls, modifies and terminates voice, video and messaging sessions between two or more participants. The related signaling servers in the architecture are referred to as Call State Control Functions (CSCFs) and distinguished by their specific functionalities. It is important to note that an IMS compliant end user system has to provide the necessary IMS protocol support, namely SIP, and the service related media codecs for multimedia applications in addition to basic connectivity support, e.g. GPRS, WLAN, etc. The IMS is designed to provide number of key capabilities required to enable new IP services via mobile and fixed networks. The important key functionalities which enable new mobile IP services are:

- Multimedia session negotiation and management
- Quality of service management
- Mobility management
- Service execution, control and interaction
- Privacy and security management

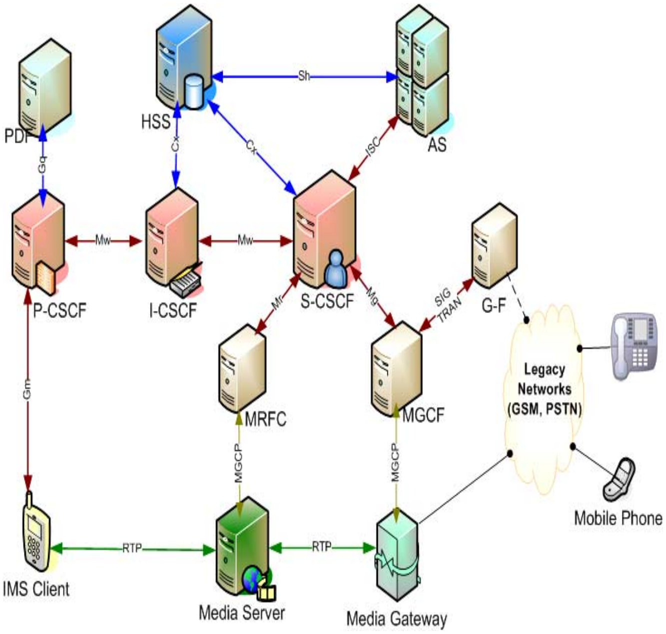

Figure 1:- IP Multimedia Subsystem (IMS) Architecture

In IMS specification, Application Server (AS) provides the service logic and service creation environment for applications and services. The AS is intended to influence and maintain the various IMS SIP sessions on behalf of the services. It can behave as a termination point for signaling, redirecting or forwarding SIP requests. It also can act as third party call control unit. Services in this instance refer to IMS services, which are based on the IMS reference points (e.g. instant messaging, presence, conferencing etc.). The advantage of application server is to enable IMS to operate in a more flexible and dynamic way, whereas the AS provides more intelligence to the system. Most Application Servers are closed boxes which map network functions (e.g. via OSA gateways) or signaling protocols (SIP) onto application programming interfaces based on a particular technology (Java, CORBA, web-services). An alternative approach pursued by the Open Mobile Alliance (OMA) is strongly related to the service oriented methodology, which follows the top-down approach beginning with service design down to service mapping over the underlying network technologies. The SIP services can be developed and deployed on a SIP application server using several technologies such as SIP servlets, Call Processing Language (CPL) script, SIP Common Gateway Interface (CGI) and JAIN APIs.

3. Generic Bootstrapping Architecture (GBA)

Different 3G Multimedia Services including video conferencing, presence, push to talk etc. has potential usage of Generic Bootstrapping Architecture (GBA) to distribute subscriber certificates. These certificates are used by mobile operators to authenticate the subscriber before accessing the multimedia services and applications. Now we discuss components, entities and interfaces of GBA.

3.1 GBA Components and Entities

The GBA consists of five entities: UE (User Equipment), NAF (Network Authentication Function), BSF (Bootstrapping Server Function) and HSS (Home Subscriber Server) and are explained below as specified in 3GPP standards (shown in figure 2).

User Equipment: UE is UICC (Universal Integrated Circuit Card) containing USIM or ISIM related information that supports HTTP Digest AKA (Authentication & Key Agreement) and NAF (Network Authentication Function) specific protocols. A USIM (Universal Subscriber Identity Module) is an application for UMTS mobile telephony running on a UICC smartcard which is inserted in a 3G mobile phone. It stores user subscriber information, authentication information and provides with storage space for text messages. An IP Multimedia Services Identity Module (ISIM) is an application running on a UICC smartcard in a 3G telephone in the IP Multimedia Subsystem (IMS). It contains parameters for identifying and authenticating the user to the IMS. The ISIM application can co-exist with SIM and USIM on the same UICC making it possible to use the same smartcard in both GSM networks and earlier releases of UMTS.

Bootstrapping Server Function (BSF): It hosts in a network element under the control of mobile network operator. The BSF, HSS, and UEs participate in GBA in which a shared secret is established between the network and a UE by running the bootstrapping procedure. The shared secret can be used between NAFs and UEs, for example, for authentication purposes. A generic Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol, and agree on session keys that are afterwards applied between UE and a Network Application Function (NAF). The BSF shall restrict the applicability of the key material to a specific NAF by using the key derivation procedure. The key derivation procedure may be used with multiple NAFs during the lifetime of the key material. The lifetime of the key material is set according to the local policy of the BSF. The BSF shall be able to acquire the GBA User security Settings (GUSS) from HSS [3].

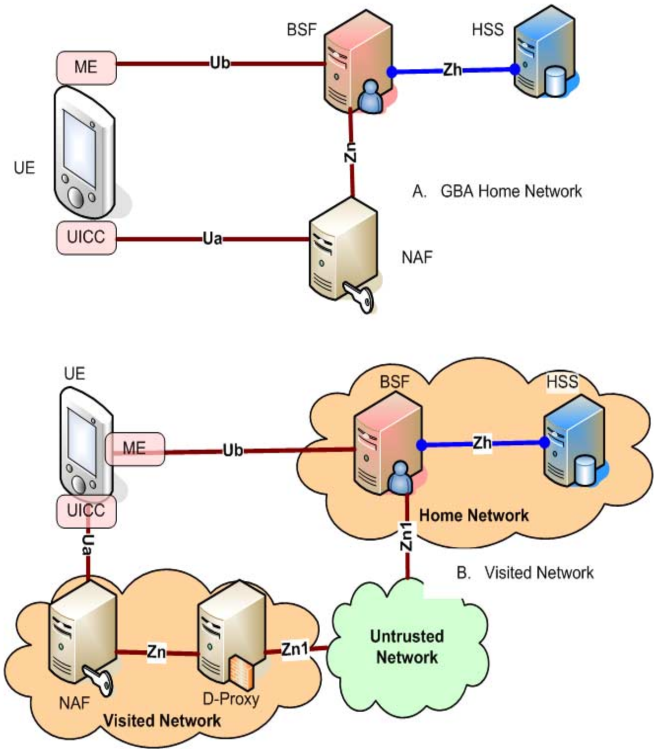

Figure 2: Network Entities of GBA

Network Authentication Function: NAF has the functionality to locate and communicate securely with subscriber's BSF (Bootstrapping Server Function). It should be able to acquire a shared key material established between the UE and the BSF during application specific protocol runs.

Home Subscriber Server: HSS stores GBA user security settings (GUSSs). The GUSS is defined in such a way that interworking of different operators for standardized application profiles is possible. It also supports operator specific application profiles without the standardized of existing application profiles. The GUSS shall be able to contain application-specific USSs that contain parameters that relates to key selection indication, identification or authorization information of one or more applications hosted by one ore more NAFs. Any other types of parameters are not allowed in the application-specific USS [3].

Diameter-Proxy: In case where UE has contacted NAF of visited network than home network, this visited NAF will use diameter proxy (D-Proxy) of NAFs network to communicate with subscriber's BSF (i.e. home BSF). D-Proxy's general functionality requirements include [3]:

- D-Proxy functions as a proxy between visited NAF and subscriber's home BSF and it will be able to locate subscriber's home BSF and communicate with it over secure channel.
- The D-Proxy will be able to validate that the visited NAF is authorized to participate in GBA and shall be able to assert to subscriber's home BSF the visited NAFs DNS name.
- The D-Proxy shall also be able to assert to the BSF that the visited NAF is authorized to request the GBA specific user profiles contained in the NAF request.

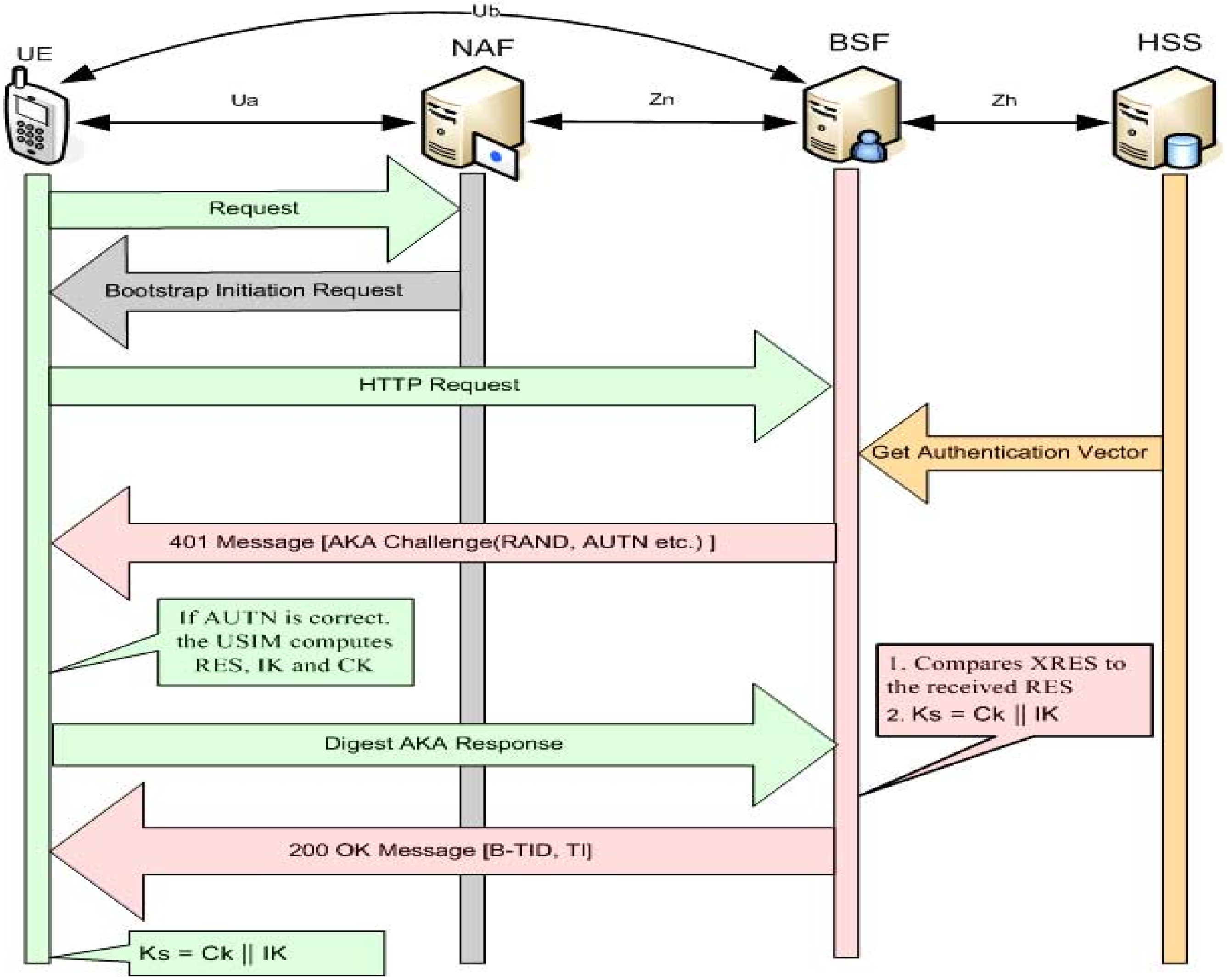
Ub
UE
NAF
BSF
HSS
Ua
Zn
Zh
Request
Bootstrap Initiation Request
HTTP Request
Get Authentication Vector
401 Message [AKA Challenge(RAND, AUTN etc.)]
If AUTN is correct, the USIM computes RES, IK and CK
1. Compares XRES to the received RES
2. Ks = Ck || IK
Digest AKA Response
200 OK Message [B-TID, Tl]
Ks = Ck || IK

Figure 3: Bootstrapping Authentication Procedure

3.2 GBA Reference Points

Ub: The reference point Ub is between the UE and the BSF and provides mutual authentication between them. It allows the UE to bootstrap the session keys based on 3GPP AKA infrastructure. The HTTP Digest AKA protocol is used on the reference point Ub. It is based on the 3GPP AKA [7] protocol.

Ua: The reference point Ua carries the application protocol, which is secured using the keys material agreed between UE and BSF as a result of running of HTTP Digest AKA over reference point Ub. For instance, in case of support for subscriber certificates, it is a protocol, which allows the user to request certificates from NAF. In this case, NAF would be PKI portal.

Zh: The reference point Zh used between BSF and HSS. It allows BSF to fetch the required authentication information and all GBA user security settings from HSS. The interface to 3G Authentication Centre is HSS-internal, and it need not be standardised as part of this architecture.

Zn: The reference point Zn is used by the NAF to fetch the key material agreed during a previous HTTP Digest AKA protocol run over the reference point Ub from the UE to the BSF. It is also used to fetch application-specific user security settings from the BSF, if requested by the NAF.

4. Bootstrapping Authentication Procedure

The UE and Network Authentication Function (NAF) have to decide whether to use GBA before the start of communication between them. When UE wants to interact with NAF, it starts communication with NAF over Ua interface without GBA parameters. If NAF requires the use of shared keys obtained by means of GBA, but the request from UE does not include GBA-related parameters, the NAF replies with a bootstrapping initiation message [3]. When UE wants to interact with NAF, and it knows that the bootstrapping procedure is needed, it shall first perform a bootstrapping authentication as shown in figure 3. Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a bootstrapping negotiation indication from the NAF, or when the lifetime of the key in UE has expired. The UE sends an HTTP request to the BSF and the BSF retrieves the complete set of GBA user security settings and one Authentication Vector (AV) [8] as given in equation 1 over the reference point Zh from the HSS.

$AV = RAND \| AUTN \| XRES \| CK \| IK$ ------------------- Eq. 1

After that BSF forwards the RAND and AUTN to the UE in the 401 message without the CK, IK and XRES. This is to demand the UE to authenticate itself. The UE checks AUTN to verify that the challenge is from an authorized network; the UE also calculates CK, IK and RES [8]. This will result in session keys IK and CK in both BSF and UE. The UE sends another HTTP request to the BSF, containing the Digest AKA response which is calculated using RES.

The BSF authenticates the UE by verifying the Digest AKA response. The BSF generates key material Ks by concatenating CK and IK and it also generates B-TID (Bootstrapping Transaction Identifier) which is used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn. The BSF shall send a 200 OK message, including a B-TID to the UE to indicate the success of the authentication and the lifetime of the key Ks. The key material Ks is generated in UE by concatenating CK and IK. Both the UE and the BSF shall use the Ks to derive the key material Ks-NAF which will be used for securing the reference point Ua. The Ks-NAF is computed as equation 2.

Ks-NAF = f_{KD}(Ks, "gba-me", RAND, IMPI, NAF-ID) ----- Eq. 2

where f_{KD} is the key derivation function and will be implemented in the ME, and the key derivation parameters consist of user's IMPI, NAF-ID and RAND. The NAF-ID consists of the full DNS name of the NAF, concatenated with the Ua security protocol identifier. The UE and the BSF shall store the key Ks with the associated B-TID for further use, until the lifetime of Ks has expired, or until the key Ks is updated [3].

5. Bootstrapping Usage Procedure

Before communication between the UE and the NAF can start, the UE and the NAF first have to agree whether to use shared keys obtained by means of the GBA. If the UE does not know whether to use GBA with this NAF, it uses the initiation of bootstrapping procedure. Once the UE and the NAF have decided that they want to use GBA then every time the UE wants to interact with NAF. The UE starts communication over reference point Ua with the NAF by supplying the B-TID to the NAF to allow the NAF to retrieve the corresponding keys from the BSF. The NAF starts communication over reference point Zn with BSF. The NAF requests key material corresponding to the B-TID supplied by the UE to the NAF over reference point Ua. With the key material request, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able to verify that NAF is authorized to use that hostname. The NAF may also request one or more application-specific USSs for the applications, which the request received over Ua from UE may access.

The BSF derives the keys required to protect the protocol used over reference point Ua from the key Ks and the key derivation parameters. Than it supplies requested key Ks-NAF, bootstrapping time and the lifetime of the key to NAF. If the key identified by the B-TID supplied by the NAF is not available at the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a bootstrapping renegotiation request to the UE. The BSF may also send the private user identity (IMPI) and requested USSs to NAF according to the BSF's policy. The NAF continues with the protocol used over the reference point Ua with the UE. Once the run of the protocol used over reference point Ua is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to use reference point Ua in a secure way.

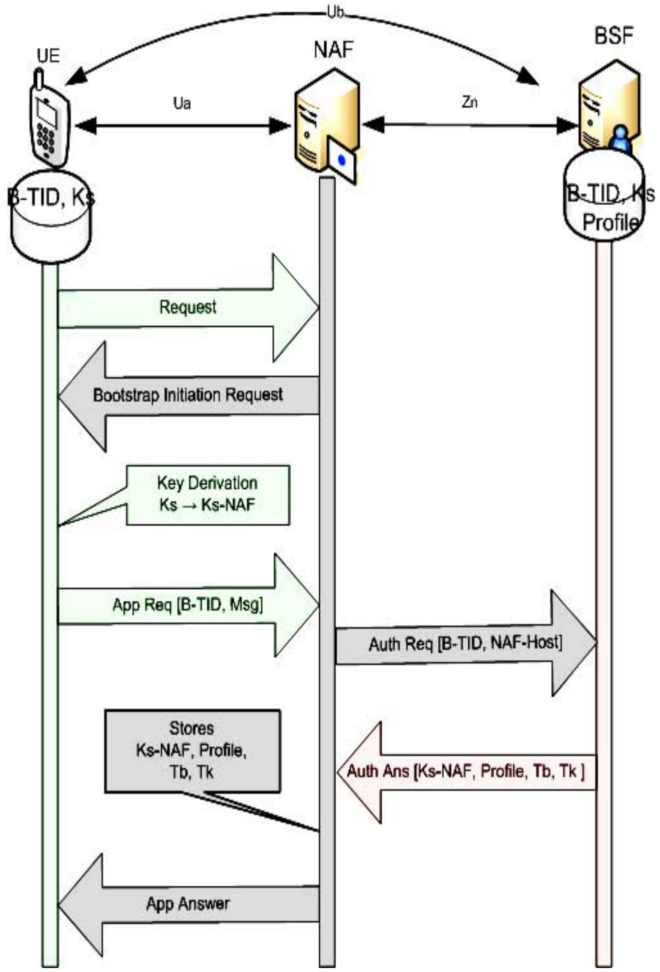

Figure 4: Bootstrapping Application

6. Authentication Proxy Usage for Multimedia Services

Authentication Proxy (AP) is like a Network Authentication Function (NAF) and performs the function of HTTP proxy for the UE. It is responsible to handle the Transport Layer Security (TLS) and implement the secure HTTP channel between AP and UE as shown in figure 5. It utilizes the 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, the AP performs UE authentication. The AP may insert the user identity when it forwards the request to application server. Figure 5b presents the architecture view of using AP for different IMS SIP services e.g. presence, messaging, conferencing etc.

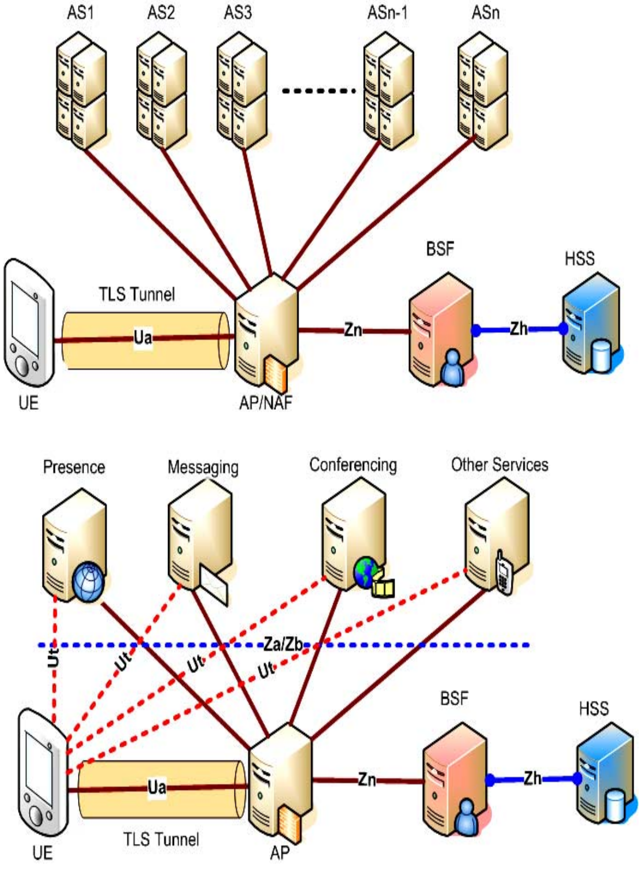

Figure 5: Authentication Proxy

The UE shall manipulate own data such as groups, through the Ua/Ut reference point [4]. The reference point Ut will be applicable to data manipulation of IMS based SIP services, such as Presence, Messaging and Conferencing services. When the HTTPS client starts communication via Ua reference point with the NAF, it shall establish a TLS tunnel with the NAF. The NAF is authenticated to the HTTPS client by means of a public key certificate. The HTTPS client will verify that the server certificate corresponds to the FQDN (Fully Qualified Domain Name) of the AP it established the tunnel with. We explain the procedure briefly as:

The HTTPS client sends an HTTP request to NAF inside the TLS tunnel. In response to HTTP request over Ua interface, the 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, the client will verify that the FDQN corresponds the AP it established the TLS connection with, if not the client will terminate the TLS connection with the AP. In this way the UE and AP are mutually authenticated as the TLS tunnel endpoints.

Now we discuss an example that 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 could establish as:

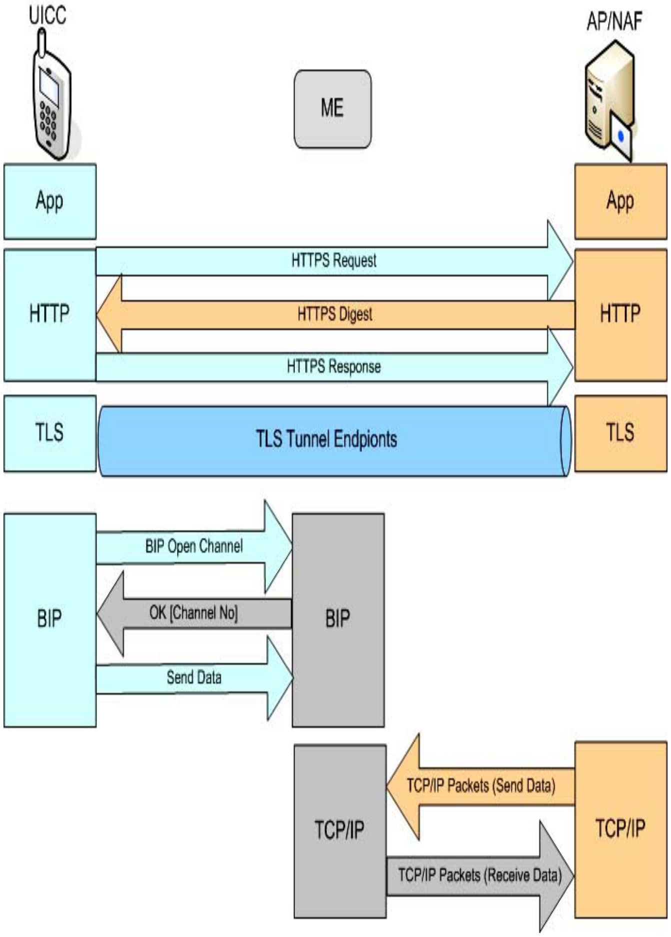

Figure 6: HTTPS and BIP (Bearer Independent Protocol) Procedures

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 [9]. Figure 6 shows the use of BIP (Bearer Independent Protocol) to establish the HTTPS connection between UICC and AP. When UICC opens channel with AP as described in [10] than an active TCP/IP connection establishes between UICC and AP.

7. Fokus IMS Testbed

In face of the current challenges within telecommunications market are mainly consequences of insufficient early access to new enabling technologies by all market players. , In this development Fraunhofer Institute FOKUS, known as a leading research institute in the field of open communication systems, has established with support of German Ministry of Education and Research (BMBF) a 3G beyond Testbed, known as “National Host for 3Gb Applications”. This Testbed provides technologies and related know-how in the field of fixed and wireless next generation network technologies and related service delivery platforms. As a part of 3Gb Testbed, the FOKUS Open IMS Playground is deployed as an open technology test field with the 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 [11]. 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 IP tunnels remotely.

Users of the “Open IMS playground” can test their components performing interoperability tests. The SIP Express Router (SER), one of the fastest existing SIP Proxies, can be used as a reference implementation and to proof interoperability with other SIP components [11]. The major focal point of IMS Playground is to put Application Server aside. Varieties of platforms enable rapid development of innovative services.

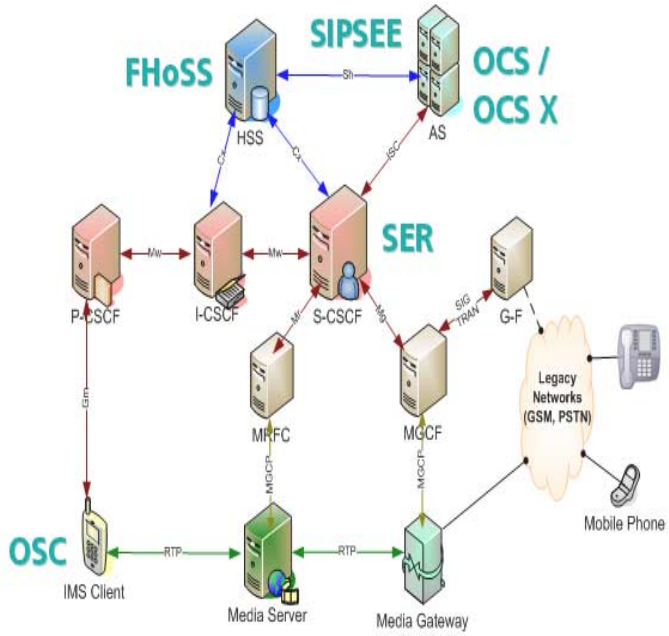

Figure 7: Fokus IMS Testbed

The Open IMS playground is deployed as an open technology test field with the target to develop prototype and validate existing and emerging NGN/IMS standard components. It extends the IMS architecture and protocols appropriately to be used on top of new access networks as well as to provide new seamless multimedia applications. It is important to stress that all components have been developed by FOKUS as reference implementations, such as an own open source IMS core system (to be publicly released in 2006 based on the famous SIP Express Router), IMS Clients and application servers (SIPSee), and HSS. The IMS playground is used on the one hand as the technology basis for own industry projects performed for national and international vendors and network operators as well as for more mid term academic R&D projects in the European IST context. In addition, the playground is used by others as well, i.e. FOKUS is providing consultancy and support services around the IMS playground. Users of the “Open IMS playground”, e.g. vendors, are testing their components performing interoperability and benchmarking tests. Application developers are developing new IMS applications based on various programming platforms provided, i.e. IN/CAMEL, OSA/Parlay, JAIN, SIP Servlets, etc., and gain a proof of concept implementation.. The different platform options, each with their strengths and weaknesses, can be selected and used according to the customers’ needs. Figure 7 displays the Open IMS playground partner components.

8. Conclusion

In this paper, we have presented the architecture of secure access and authentication of IP Multimedia Services based of SIP and HTTP communication using GBA (Generic Bootstrapping Architecture) as recommended by 3GPP and TISPAN as a part of Secure Service Provisioning (SSP) Framework of IMS at Fokus Fraunhofer IMS and 3Gb Testbed.

9. REFERENCES

[1] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; TS 23.228 IP Multimedia Subsystem (IMS), Stage 2 / 3GPP2 X.S0013-002-0 v1.0, www.3gpp.org.

[2] ETSI TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking) WG http://portal.etsi.org/tispan/TISPAN_ToR.asp.

[3] 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).

[4] 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).

[5] Third Generation & Beyond (3Gb) Testbed, www.fokus.fraunhofer.de/national_host &

IP Multimedia System (IMS) Playground www.fokus.fraunhofer.de/ims.

[6] M. Sher, T. Magedanz, “Secure Service Provisioning Framework (SSPF) for IP Multimedia System and Next Generation Mobile Networks” 3rd International Workshop in Wireless Security Technologies, London, U.K. (April 2005), IWWST’05 Proceeding (101-106), ISSN 1746-904X.

[7] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 6); 3GPP, TS 33.102 V6 (2004).

[8] 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 LNCS 3744-0263, Berlin

Heidelberg 2005, pp. 263-272. http://www.congresbcu.com/mata2005

[9] Third Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Early Implementation of HTTPS Connection between a Universal Integrated Circuit Card (UICC) and Network Application Function (NAF) (Release 7), 3GPP TR 33.918 V7 (2005).

[10] Third Generation Partnership Project; Technical Specification Group Core Network and Terminals; Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (Release 7), 3GPP TS 31.111 V7 (2005).

[11] K. Knüttel, T.Magedanz, 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.

10. Acronyms

3GPP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authentication, Authorisation, and Accounting
AKA	Authentication and Key Agreement
AP	Authentication Proxy
AS	Application Server
AuC	Authentication Centre
AV	Authentication Function
BGA	Generic Bootstrapping Architecture
BSF	Bootstrapping Server Function
B-TID	Bootstrapping Transaction Identifier
CAMEL	Customized Applications for Mobile Enhanced Logic
CGI	Common Gateway Interface
CK	Cipher Key
CORBA	Common Object Request Broker Architecture
CPL	Call Programming Language
CSCFs	Call State Control Functions
DNS	Domain Name Server
FMC	Fixed Mobile Convergence
FQDN	Fully Qualified Domain Name
GAA	Generic Authentication Architecture
GPRS	General Packet Radio System
GUSS	GBA User Security Settings
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP – Secure (HTTP over TLS)
ICSCF	Interrogating Call State Control Function
IETF	Internet Engineering Task Force
IK	Integrity Key
IM	IP Multimedia
IMPI	IP Multimedia Private Identity
IMS	IP Multimedia Subsystem
IN	Intelligent Network
IP	Internet Protocol
ISIM	IM Service Identity Module
Ks	Session Key
ME	Mobile Equipment
MG	Media Gate
MRF	Media Resource Function
NAF	Network Authentication Function
NGN	Next Generation Network
OMA	Open Mobile Alliance
OSA	Open Service Access
PCSCF	Proxy Call State Control Function
PDP	Packet Data Protocol
PoC	PPT over Cellular
PTT	Push To Talk
QoS	Quality of Service
RES	Response
RTP	Real-time Transport Protocol
SCSCF	Serving Call State Control Function
SDP	Service Delivery Platform
SER	SIP Express Router
SIP	Session Initiation Protocol
SSP	Secure Service Provisioning
TCP	Transmission Control Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TLS	Transport Layer Security
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication Standard
USIM	Universal Subscriber Identity Module
WLAN	Wireless Local Area Network