



SECURE MOBILE COMMUNICATIONS WITH IMS AKA SIGNALING

Authors:

Paul Wilgosiewicz and Scott Poretsky

June 15, 2007

About the IMS Forum:

The IMS Forum is a global, non-profit industry association devoted to interoperable IP Multimedia Subsystems services and solutions. Their mission is to accelerate the adoption of IMS through discussion and resolution of interoperability issues and the development of standards-based IMS services residing in the IMS application layer. The Forum also provides consultancy to industry service providers and vendors on best practices and approaches for IMS rollouts and interconnectivity. The IMS Plugfest facilitates the industry-wide certification of applications and services interoperability. More information is available at www.imsforum.org

About the Authors:

Paul Wilgosiewicz has been employed Motorola Labs since 2001 providing support for leading edge telecommunications research projects. Paul specializes in network architectures and has designed and configured numerous VoIP test beds. Paul earned his bachelors degree in computer science at Roosevelt University and his master's degree in Information Technology Management from the Illinois Institute of Technology.

Scott Poretsky is director of carrier network engineering at Reef Point Systems and is currently serving as Technical Chair of the IMS Forum. Prior to Reef Point, Scott contributed to leading edge carrier product development at Avici Systems and General DataComm. He is a member of the IEEE and an active participant in its Communications Quality and Reliability (CQR) committee. Scott has authored numerous IETF standards for IP performance benchmarking and has been awarded one patent for networking technology. He earned his BSEE at the University of Vermont and MSEE at Worcester Polytechnic Institute.

Table of Contents

References	3
Glossary.....	4
Executive Summary	5
1.0 Introduction	6
2.0 3GPP IMS Overview.....	7
2.1 3GPP IMS Architecture Overview	7
2.2 3GPP SIP Message Headers.....	8
3.0 Registration with AKA Signaling	9
4.0 HSS Authentication of the UE.....	11
5.0 Security with a Border Gateway Function (BGF)	12
6.0 Conclusions	13
Appendix 1 SIP REGISTER Header Examples	14

References

- [1] 3GPP TR 21.801: "Technical Specification Group Services and System Aspects; Specification drafting rules"
- [2] 3GPP TS 11.11: "Technical Specification Group Terminals Specification of the Subscriber Identity Module -Mobile Equipment (SIM- ME)"
- [3] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the IP Multimedia Core Network".
- [4] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".
- [5] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".
- [6] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".
- [7] 3GPP TS 31.101: "Technical Specification Group Core Network and Terminals; UICC-terminal interface; Physical and logical characteristics"
- [8] 3GPP TS 31.102: "Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application"
- [9] 3GPP TS 31.103: "Technical Specification Group Core Network and Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application"
- [10] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".
- [11] 3GPP TS 33.203: " Technical Specification Group Services and System Aspects 3G security Access security for IP-based services"
- [12] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".
- [13] IETF RFC 3261 "SIP: Session Initiation Protocol".
- [14] ETSI ES 282 003 "Border Gateway Functions".
- [15] ETSI TS 183 021 "NGN Release 1 - Endorsement of 3GPP TS 29.162 Interworking between IM CN Sub-system and IP networks"

Glossary

AUTN	AUthentication TokeN
AKA	Authentification and Key Agreement
AOR	Address of Record
BGCF	Breakout Gateway Control Function
CK	Cipher Key
CN	Core Network
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FQDN	Fully-Qualified Domain Name
GPRS	General Packet Radio Service
HN	Home Network
HSS	Home Subscriber Server
I-CSCF	Interrogating-CSCF
IK	Integrity Key
IM	IP Multimedia
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ISIM	IM Services Identity Module
K	long-term secret Key shared between the ISIM and the AuC
MGCF	Media Gateway Control Function
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PDP	Packet Data Protocol
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAND	RANdOm challenge
RES	user RESponse
S-CSCF	Serving-CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SQN	SeQuence Number
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
USIM	User Service Identity Module
VN	Visited Network
XRES	eXpected user RESponse

Executive Summary

The Third Generation Partnership Project (3GPP) is the standards body for the IP Multimedia Subsystem (IMS) architecture to deliver reliable and seamless mobile services to users on any access network (such as WiFi, WiMax, Femtocell, cellular, etc.). The protocol selected for service delivery is the Session Initiation Protocol (SIP), as standardized by the Internet Engineering Task Force (IETF). SIP can be used for delivery of Internet Protocol (IP) services such as Voice over IP (VoIP) and Instant Messaging (IM). Unfortunately, due to SIP's loose requirements it is unable to provide a reliable and secure connection. Several functional entities and mechanisms are required to meet the needs of service providers deploying IMS. One of these mechanisms is the Authentication and Key Agreement (AKA) signaling method [11]. Its purpose is to guarantee a secure and confidential SIP connection from the mobile user equipment (UE) to the IMS home network (HN). AKA is an extension to the SIP protocol based upon the 3GPP SIP [6] which is based upon the IETF SIP [13], but uses modified headers and messaging sequencing.

With AKA, the IMS network issues a challenge when a UE attempts to REGISTER. If the user is authorized access by the HN, then keys are exchanged, the UE and IMS network mutually authenticate, an IPsec transport tunnel is established from the UE to the IMS network, and Registration is completed with encrypted SIP signaling. The IP transport tunnel remains established and all SIP signaling for session establishment is encrypted through the tunnel. A major advantage of the AKA signaling to the user and IMS provider is mutual authentication, service authorization, and confidentiality while the off-net user is accessing services from a visited network (VN).

AKA requires support at the UE, P-CSCF, I-CSCF and S-CSCF. The UE and P-CSCF also require support for IPsec transport mode and encryption/ decryption. It is possible to deploy the P-CSCF in a configuration so that a Border Gateway Function (BGF) terminates the IPsec tunnel with the UE, encrypts/decrypts SIP messages destined for the P-CSCF, and participates in the key exchange with the P-CSCF. The S-CSCF has the critical role in AKA signaling to make the authorization decision based upon a lookup to the Home Subscriber Server (HSS).

1.0 Introduction

The Third Generation Partnership Project (3GPP) is the standards body for the IP Multimedia Subsystem (IMS) architecture to deliver reliable and seamless mobile services to users on any access network (such as WiFi, WiMax, Femtocell, cellular, etc.). The protocol selected for service delivery is the Session Initiation Protocol (SIP), as standardized by the Internet Engineering Task Force (IETF). The registration process is the core method that divides the IETF and 3GPP architectures. Registration standardized by the IETF, is an optional process that creates a binding between the Address of Record (AOR) and the current Uniform Resource Identifier (URI). This enables subscribers to contact each other, without prior contact information. However, registration for the IMS architecture is mandatory and has numerous requirements. This process creates an AOR / URI binding and requires mutual authentication that is protected by an encrypted tunnel setup following a key agreement procedure. This entire process is called IMS AKA. IMS AKA is a two stage process. The first stage setups the encrypted tunnel. The second stage authenticates the home network and UE, and creates a binding between the subscribers AOR and current URI is established. This procedure not only protects the registration messages, subsequent packets are also protected for the duration of the registration. The IMS architecture has achieved this by utilizing numerous required SIP header fields and functional entities.

The IMS architecture mandates that numerous header fields are used to transfer essential data. These header fields are available in the IETF standard, but they are only optional. Utilizing these headers enables SIP to transmit the subscriber's private user identity, supported algorithms, encryption keys, challenge request and response, identity of the visited network, and charging vectors. These key pieces of information allow the service providers the ability to ensure a secure connection and collect usage information for billing. Usage information is essential to service providers so that they can charge their subscribers appropriately. IMS does not specify how service providers charge, it only enables them to do so. These required header fields are necessary to transfer data between the home network (HN) and UE.

The SIP messages must traverse numerous required functional entities that parse the messages and extract and add data. These functional entities are not standardized by the IETF and only exist in the IMS architecture. The core entities are Home Subscriber Server, and the Call Session Control Functions, which consist of a Proxy, Interrogating, and Serving. Each of the functional entities is essential to provide a secure and authenticated connection.

The remaining sections of this document discuss the 3GPP IMS architecture, 3GPP SIP messaging, and 3GPP AKA signaling in detail. Appendix 1 provides example packet decodes used for AKA signaling in the IMS core network.

2.0 3GPP IMS Overview

2.1 3GPP IMS Architecture Overview

The IMS Architecture is designed to deliver applications to users on any access network through a common IMS core network. This enables new services to be rolled-out and existing services to be upgraded without impact to the core network. The IMS core components that participate in mutual authentication of a UE are P-CSCF, I-CSCF, S-CSCF, and HSS. Figure 1 shows these components and the interfaces between them. The HSS is a database where the subscribers profile is stored, which includes authentication data and services available to the subscriber. The P-CSCF functions as the UE's first point of contact. An encrypted tunnel is constructed between the UE and the P-CSCF during the IMS AKA. The I-CSCF functions as the HN's first point of contact from the visited networks P-CSCF.

When a registration request is received by I-CSCF, a query is sent to the HSS, to validate the request and determine which S-CSCF the registration should be forwarded to. Once an S-CSCF is selected, it will remain in the SIP message path for the duration of the registration period. The S-CSCF may forward SIP messages to Application Servers that the users subscribers to. This layered approach allows for rapid integration of new services and features. These services are not limited to the subscriber's service provider; they may include third parties provided services. Since the P-CSCF and S-CSCF remain in the signaling path they can be used to collect usage data by both the visited and home networks. The Gm interface extends from the UE through the access network to the P-CSCF. It is over this interface that IPsec is established between the UE and P-CSCF. Communication between the CSCFs occurs over the Mw interface and Communication between the CSCFs and HSS occurs over the Cx interface. The AKA signaling that is performed over these interfaces for mutual authentication of the UE and network is discussed in subsequent sections.

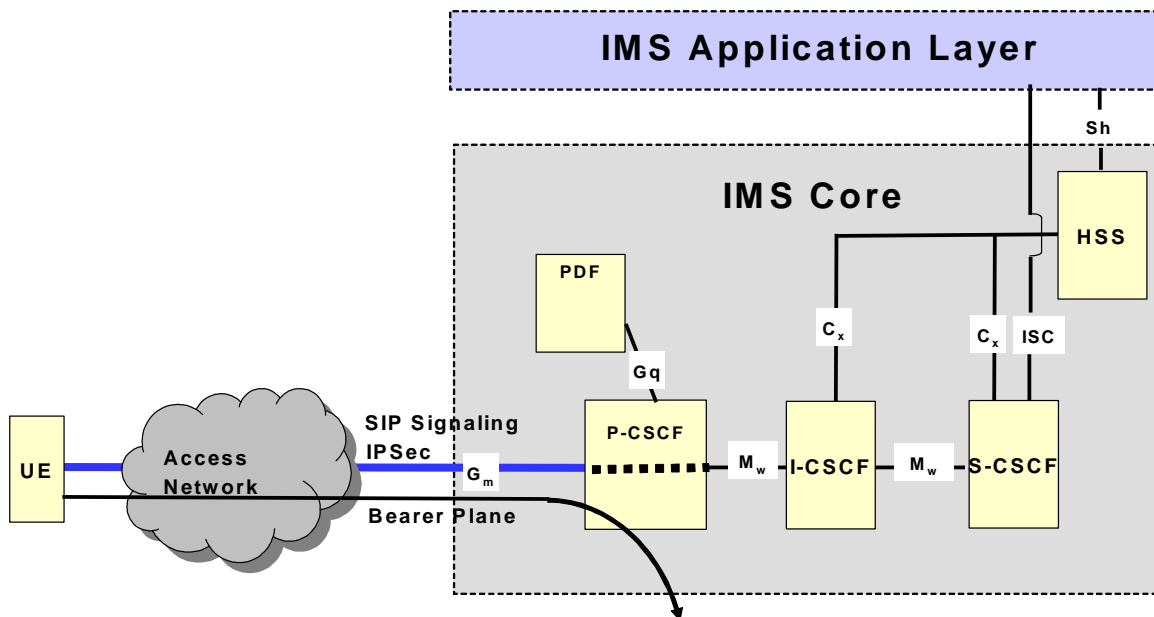


Figure 1. 3GPP IMS Architecture for AKA Signaling

2.2 3GPP SIP Message Headers

IMS is based upon the IETF's SIP RFC 3261 [13]. The message types are the same, with the exception of required header fields. IMS uses the same set of METHODS and Response Types as IETF SIP. 3GPP TS 24.229 [6], Appendix B.1 provides a table of the methods supported by the IETF and 3GPP. 3GPP TS 24.229, Appendix B.2 provides a table of Response Types supported by the two organizations. One difference between the IETF and 3GPP implementation of SIP is the optional IETF registration headers that are required in IMS. These are Request-URI, To, From, Call-ID, CSeq, Contact, Via, Authorization. These headers are required in IMS to provide a secure and mutually authenticated connection. These headers are discussed in more detail in Figure 2.

Required IMS Registration Headers	
Request-URI:	→ This is the URI of the domain the registration request is being sent to. Example: Request-URI:<sip:homedomain.com>
To:	→ This header must contain the users Address-of-Record. Example: To: <sip:paul@homedomain.com>
From:	→ This header contains the Public User Identity or Address-of-Record of the person who generated the registration request. Most often this will be the same as the To: header. Example: From:<sip:paul@homedomain.com>
Call-ID:	→ This is unique identifier assigned by the client. To ensure uniqueness the identifier should included the domain name of the client. All registration request sent to the SIP server should use the same Call-ID. Example: Call-ID:s234ttg9f445oitu@pc1.home.com
CSeq:	→ This header contains the method name and sequence number of the request. The SIP client must increment the number every time a registration request is sent with the same Call-ID. Example: CSeq: 1 REGISTER
Contact:	→ This header contains the current contact URI for the client. This header is required in the IMS Architecture. Example: Contact: <sip:paul@pc1.home.com>
Via:	→ This header records the SIP URI of every entity that processes the request. Example: Via: pc1.home.com:5060;branch=z9hG4bK
Authorization:	→ This provides the home network the subscribers Private User Identity. Example: Authorization: Digest username="12345_private@homedoamin.com", realm="homedomain.com", nonce="", uri="sip:homedomain.com", response=""

Figure 2. Required IMS Registration Headers

3.0 Registration with AKA Signaling

The primary difference between the IETF and 3GPP implementation of SIP is the signaling to support AKA [5][11]. The registration process is one of the core methods that divide the IETF and 3GPP architectures. IETF's registration process creates a binding between the AOR and the current URI. This enables subscribers to contact the each other, without prior contact information. Registration in the IMS architecture is mandatory. This process creates a binding and also requires mutual authentication and key agreement procedure to setup an encrypted tunnel. This process is called IMS AKA. IMS AKA is a two stage process. The first stage establishes the encrypted tunnel. The second stage authenticates the home network and UE, and creates a binding between the subscribers AOR and current URI is established. Figure 3 shows the two phases of the 3GPP IMS Registration Process with AKA Signaling through the Visited and Home Networks. This involves the following steps:

PHASE 1 REGISTRATION:

1. **IMS Mobile Handset (known as the User Equipment – UE) sends a SIP REGISTER message in the clear (unencrypted) to a known P-CSCF IP address.** If this initial SIP REGISTER message is encrypted then it should be dropped at the P-CSCF.
2. **Upon receiving a SIP REGISTER message in the CLEAR, the P-CSCF determines if this subscriber is on his Home Network or a Visited Network.**
3. **If the subscriber is on a Visited Network then the P-CSCF forwards the REGISTER message to the I-CSCF of the subscriber's Home Network. The I-CSCF forwards the message to the S-CSCF. If the subscriber is on his Home Network then the REGISTER is sent directly to the S-CSCF.**
4. **The S-CSCF upon receipt of the REGISTER message authenticates the subscriber at the HSS and returns.a 401 UNAUTHORIZED RESPONSE to the UE.**
5. **Upon receiving the challenge in the 401 UNAUTHORIZED RESPONSE, the UE then authenticates the network and establishes an IPsec transport mode tunnel with the P-CSCF . This completes Phase 1 of the Registration.**

PHASE 2 REGISTRATION:

6. **Once IPsec is established, the UE sends a second REGISTER message that is encrypted through the IPsec tunnel to the known P-CSCF.** If the SIP REGISTER is in the clear then it should be dropped at P-CSCF.
7. **SIP Registration is completed when the S-CSCF returns a 200 OK message to the UE.**

Registration Message Sequence

IMS Registration is a two stage process that requires mutual authentication and setups IPsec tunnel between the UE and P-CSCF.

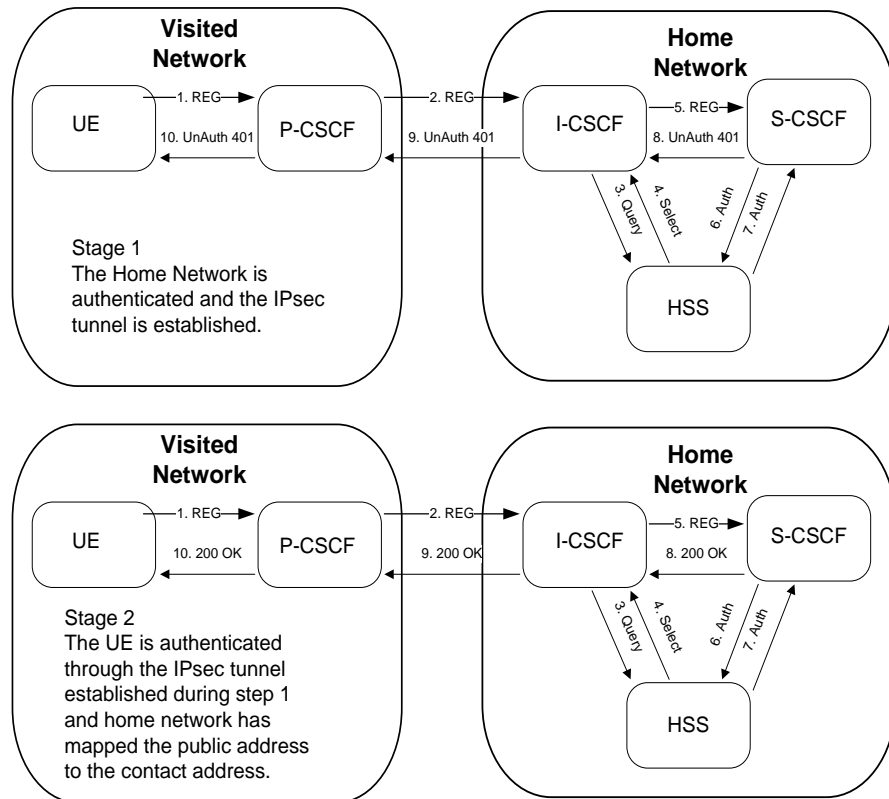


Figure 3. 3GPP IMS Registration Process with AKA Signaling

It is important to note the following regarding IPsec:

1. The IPsec is terminated at the UE and P-CSCF. The P-CSCF performs encryption and decryption so that the I-CSCF and S-CSCF process SIP messages in the clear.
2. All SIP messaging after successful Registration, including INVITES to establish calls, is encrypted to/from the UE through the IPsec tunnel. The 3GPP session initiation process is very similar with a couple notable differences. These differences enable both the VN and HN to collect usage data for IP billing.
3. Only SIP signaling messages are encrypted through the IPsec tunnel. RTP media streams flow in clear from the UE.

The message sequence between the UE and the IMS Core functional entities during the registration and session establishment process illustrate how 3GPP provides carrier grade service. The registration process executes mutual authentication between the UE and the P-CSCF. This process also delivers the required keys to create an encrypted transport between the UE and P-CSCF. The Policy Decision Function (PDF) is also invoked during this process to allocate bandwidth to the UE. Confidentiality of subsequent sessions will be ensured via the encrypted tunnel.

4.0 HSS Authentication of the UE

Before the registration can begin, the UE and HSS in the home network need to be provisioned with the subscriber's information. The UE's ISIM and HN's HSS must at a minimum contain the following data: private user identity, public user identity, home domain, and long-term shared secret key. This data is essential to the registration procedure. The UE then needs to obtain IP connectivity and discover the P-CSCF in the network. In the cases where GPRS is used, this can be established during the Packet Data Protocol (PDP) context activation. This activation process obtains an IP address, discovers the P-CSCF, and communicates with the Policy Decision Function to allocate bandwidth for the UE. Once those prerequisites are fulfilled, the UE is ready to begin the registration request. Figure 4 shows the keying for mutual authentication of the UE and HSS at the Home Network.

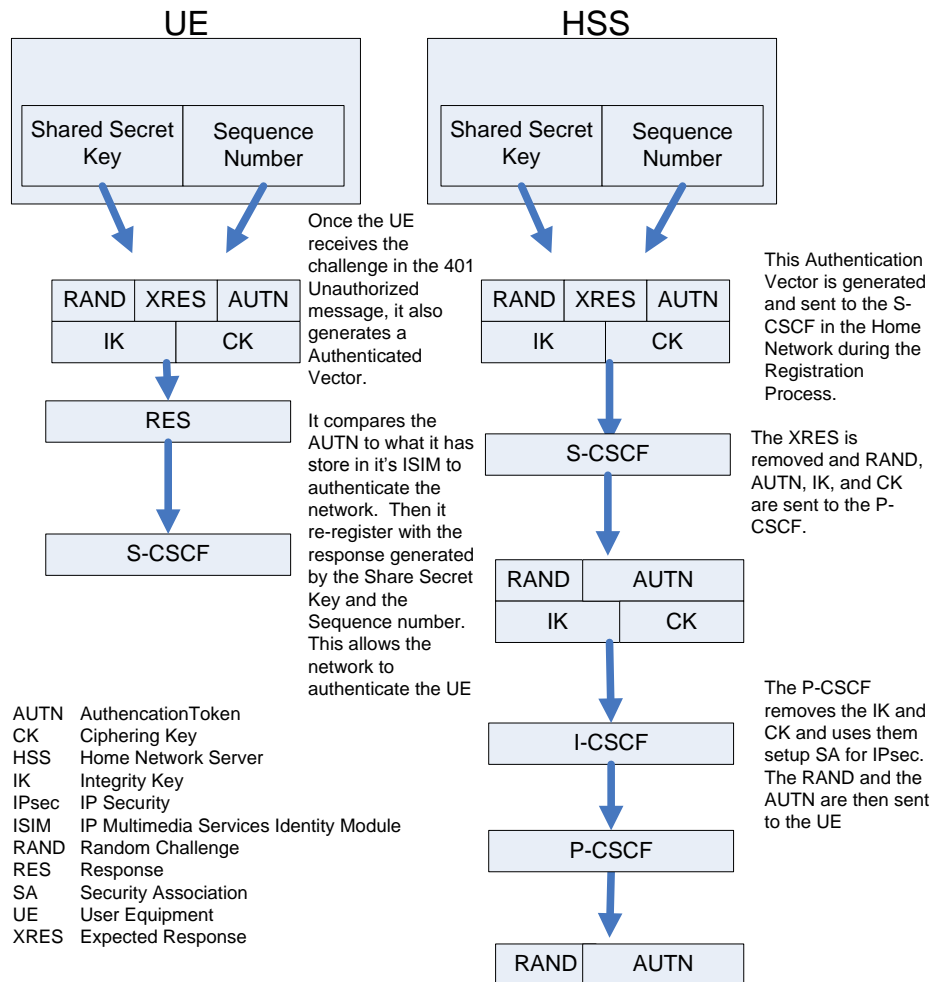


Figure 4. Keying for HSS Authentication of the UE

5.0 Security with a Border Gateway Function (BGF)

Some IMS network architectures have modified the 3GPP IMS to incorporate the Border Gateway Function (BGF) from TISpan IMS [15]. The BGF sits between the access network and P-CSCF so that the access security and policy enforcement is offloaded from the P-CSCF. This enables the P-CSCF to maintain 3GPP SIP processing performance and the specialized BGF hardware to terminate IPsec tunnels at scale with per-session and per-flow policy enforcement. Figure 5 shows the IMS architecture modified with the BGF terminating the Gm interface and signaling with the P-CSCF over the Zb interface. This architecture requires modification to the AKA signaling described in section 3 so that

- the BGF terminates IPsec with the UE
- the BGF decrypts/encrypts SIP traffic to/from the P-CSCF
- the BGF dynamically opens a SIP and Media Pinholes in its SIP ALG for authorized sessions
- the BGF performs NAT on the SIP and RTP using its NAT ALG
- the BGF enforces per-flow QoS policies on associated media

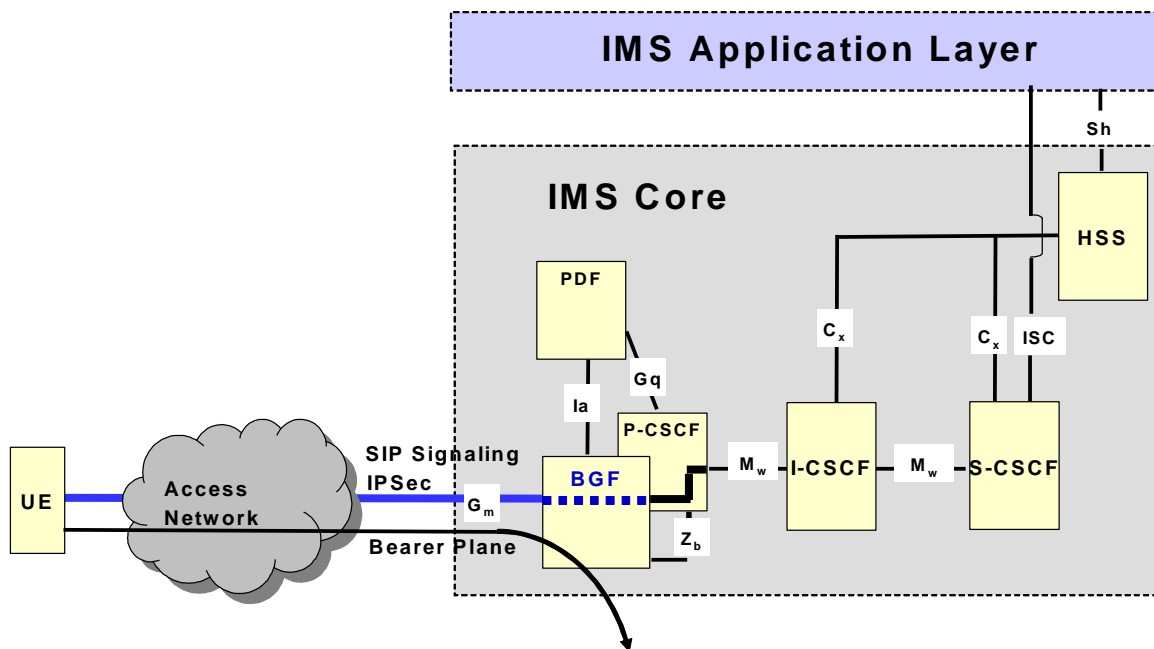


Figure 5. 3GPP IMS Architecture with TISpan BGF

6.0 Conclusions

Several functional entities and mechanisms are required to meet the needs of service providers deploying IMS. One of these mechanisms is the Authentication and Key Agreement (AKA) signaling method. Its purpose is to guarantee a secure and confidential SIP connection from the mobile user equipment (UE) to the IMS home network (HN). AKA is an extension to the SIP protocol based upon the 3GPP SIP which is based upon the IETF SIP, but uses modified headers and messaging sequencing. With AKA, the IMS network issues a challenge when a UE attempts to REGISTER. If the user is authorized access by the HN, then keys are exchanged, the UE and IMS network mutually authenticate, an IPsec transport tunnel is established from the UE to the IMS network, and Registration is completed with encrypted SIP signaling. The IP transport tunnel remains established and all SIP signaling for session establishment is encrypted through the tunnel. A major advantage of the AKA signaling to the user and IMS provider is mutual authentication, service authorization, and confidentiality while the off-net user is accessing services from a visited network (VN). AKA requires support at the UE, P-CSCF, I-CSCF and S-CSCF. The S-CSCF has the critical role in AKA signaling to make the authorization decision based upon a lookup to the Home Subscriber Server (HSS). The UE and P-CSCF also require support for IPsec transport mode and encryption/ decryption. It is possible to deploy the P-CSCF in a configuration so that a Border Gateway Function (BGF) terminates the IPsec tunnel with the UE, encrypts/decrypts SIP messages destined for the P-CSCF, and participates in the key exchange with the P-CSCF.

Appendix 1 SIP REGISTER Header Examples

These examples have been provided by 3GPP TS 24.228. The examples only illustrate the headers that have been altered by the entity. Unaltered headers are left blank.

Packet 1: REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd];comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net",
    realm="registrar.home1.net", nonce="", uri="sip:registrar.home1.net", response=""
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678;
    port-c=2468; port-s=1357
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 1 REGISTER
Supported: path
Content-Length: 0
```

Packet 2: REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net",
    realm="registrar.home1.net", nonce="", uri="sip:registrar.home1.net",
    response="", integrity-protected="no"
CSeq:
Supported:
Content-Length:
```

Packet 3: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info:
Path:
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Supported:
Content-Length:
```

Packet 4: 401 Unauthorized response (S-CSCF to I-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>; tag=5ef4
Call-ID: apb03a0s09dkjdfg1kj49111
WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN +
    server specific data), algorithm=AKAv1-MD5,
    ik="00112233445566778899aabbccddeeff", ck="ffeeddccbaa11223344556677889900"
CSeq: 1 REGISTER
Content-Length: 0
```

Packet 5: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
WWW-Authenticate:
CSeq:
Content-Length:
```

Packet 6: 401 Unauthorized response (I-CSCF to P-CSCF)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
WWW-Authenticate:
CSeq:
Content-Length:
```

Packet 7: 401 Unauthorized response (P-CSCF to UE)

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd];comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
WWW-Authenticate: Digest realm="registrar.home1.net", nonce=base64(RAND + AUTN +
server specific data), algorithm=AKAv1-MD5
Security-Server: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-
s=87654321; port-c=8642; port-s=7531
CSeq:
Content-Length:
```

Packet 8: REGISTER request (UE to P-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>;tag=4fa3
To: <sip:user1_public1@home1.net>
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
Call-ID: apb03a0s09dkjdfglkj49111
Authorization: Digest username="user1_private@home1.net",
realm="registrar.home1.net", nonce=base64(RAND + AUTN + server specific data),
algorithm=AKAv1-MD5, uri="sip:registrar.home1.net",
response="6629fae49393a05397450978507c4ef1"
Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=23456789; spi-s=12345678;
port-c=2468; port-s=1357
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-
s=87654321; port-c=8642; port-s=7531
Require: sec-agree
Proxy-Require: sec-agree
CSeq: 2 REGISTER
Supported: path
Content-Length: 0
```

Packet 9: REGISTER request (P-CSCF to I-CSCF)

```
REGISTER sip:registrar.home1.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Path: <sip:term@pcscf1.visited1.net;lr>
Require: path
P-Visited-Network-ID: "Visited Network Number 1"
P-Charging-Vector: icid-value="AyretyU0dm+6O2Irt5tAFrbHLso=023551024"
From:
To:
Contact:
Call-ID:
Authorization: Digest username="user1_private@home1.net",
realm="registrar.home1.net", nonce=base64(RAND + AUTN + server specific data),
algorithm=AKAv1-MD5, uri="sip:registrar.home1.net",
response="6629fae49393a05397450978507c4ef1", integrity-protected="yes"
CSeq:
Supported:
Content-Length:
```

Packet 10: REGISTER request (I-CSCF to S-CSCF)

```
REGISTER sip:scscf1.home1.net SIP/2.0
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
P-Access-Network-Info:
Path:
Require:
P-Visited-Network-ID:
P-Charging-Vector:
From:
To:
Contact:
Call-ID:
Authorization:
CSeq:
Supported:
Content-Length:
```

Packet 11: 200 OK response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf1_p.home1.net;branch=z9hG4bK351g45.1, SIP/2.0/UDP
    pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Path: <sip:term@pcscf1.visited1.net;lr>
Service-Route: <sip:orig@scscf1.home1.net;lr>
From:
To:
Call-ID:
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>;expires=600000
CSeq:
Date: Wed, 11 July 2001 08:49:37 GMT
P-Associated-URI: <sip:user1_public2@home1.net>, <sip:user1_public3@home1.net>,
    <sip:+1-212-555-1111@home1.net;user=phone>
Content-Length:
```

was successful.

Packet 12: 200 OK response (I-CSCF to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
    [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Path:
Service-Route:
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```

Packet 13: 200 OK response (P-CSCF to UE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Path:
Service-Route:
From:
To:
Call-ID:
Contact:
CSeq:
Date:
P-Associated-URI:
Content-Length:
```