Alcatel·Lucent

TECHNOLOGY WHITE PAPER

IMS Interconnect: Peering, Roaming and Security – Part Two

IMS interconnection promises to enable greater reach and richer offerings for the providers that establish successful peering arrangements.

This paper provides an introduction to IMS interconnection and identifies security considerations that carriers must address in order to achieve the proper balance of providing access while maintaining security.

The paper is organized into two parts – Part One introduces key concepts and definitions related to network interconnections and interconnect models, while Part Two addresses the security mechanisms within the IMS standards and identifies potential security threats that face IMS carriers looking to interconnect their networks.

Introduction

Part One of this white paper introduced concepts related to the interconnection of IMS networks, including a discussion of a variety of peering and roaming scenarios.

Part Two will describe the basic IMS security functions defined by the standards organizations, and it will describe how those functions would apply to an IMS interconnect scenario.

Table of Contents

1 Basic IMS Security Concepts and Facilities

2 Security Association 1 & 2 Overview – Subscriber to IMS

3 Security Association 4 Overview – Visited P-CSCF to home I-CSCF & S-CSCF

4 Security Association 6 & 7 Overview – IMS Network to IMS Network

5 Session Border Controllers

6 Detailed Call Flow for Interconnect Scenario & Identification of Potential Vulnerabilities

8 Recap of the Key Requirements

9 Conclusion – Looking Forward

9 References

10 List of Acronyms

11 Acknowledgements

11 About the Author

Basic IMS Security Concepts and Facilities

In the traditional telephony world, much of the security of the PSTN lies in the lack of accessibility to key portions of the network. While it is fairly easy to tap a single telephone line, to do so requires physical access to that line. Once the access is obtained, the reward is limited – essentially the tapper can initiate calls or eavesdrop on calls in progress, but the activities are limited to the constraints of that line. Obtaining access to the PSTN core infrastructure however is, by design, much more complicated. Operators of the PSTN make an assumption that sessions operating on the core network are legitimate, authorized sessions, and that the source and destination of the traffic is known. This assumption is reflected in the design and operation of the equipment that makes up the PSTN. This is in direct contrast with the IMS architecture, where the open nature of TCP/IP networking makes these assumptions impossible.

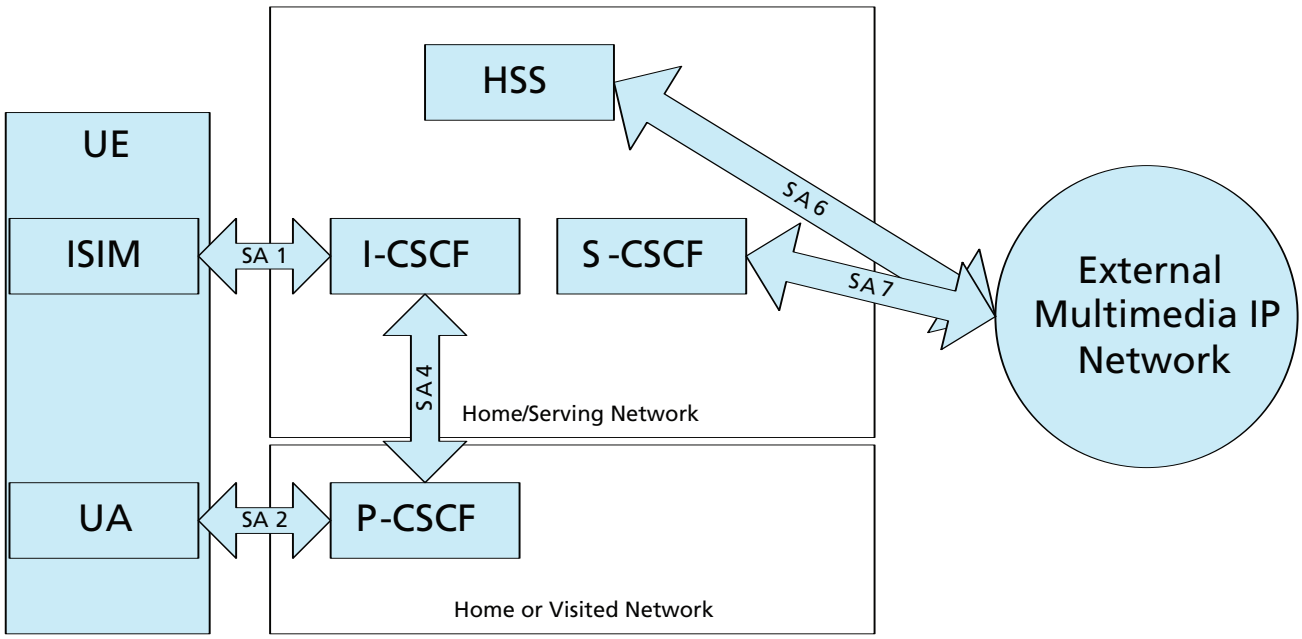
To address the need for secure IMS communications, 3GPP and 3GPP2 developed a series of security specifications. These specifications identify sets of requirements (referred to as Security Associations (SAs) that define the security provisions that apply to connections between elements within the IMS architecture. Security between the access network and the IMS network are defined in TS 33.203, and access between IMS core networks (Network Domains) is defined in TS 33.210 [1, 2].

Security within the IMS model is defined on a "hop by hop" basis, to provide for security on the links between any elements in the architecture. In situations where the connections between elements will occur outside of the IMS core, there are more extensive security requirements defined. For example, the security provisions for the connection between a UE and a P-CSCF are based on the assumption that this connection may take place over a non-secured, untrusted IP access network, while communications between elements such as the HSS and the S-CSCF are occurring over a more secure, core network that is managed by the carrier.

The most relevant SAs for IMS interconnect scenarios are: SAs 1&2 — which define the security facilities for authentication of the UE to the IMS network, SA 4, which defines security for the connection between a visited P-CSCF and the home I-CSCF & S-CSCF and SAs 6&7 which define the security facilities for connections between IMS networks (described only in 3GPP2 S.S0086-B)[3].

Figure 1 shows a simplified view of the elements and the SA that apply to the links between these elements.

FIGURE 1 – Simplified view of the IMS Security Architecture



Security Association 1 & 2 Overview – Subscriber to IMS

Part One of this paper described the process for a UE to locate a P-CSCF, but there are additional activities required for the UE to connect to and authenticate with its home IMS. These activities are governed by Security Associations 1&2.

Security Association 1 addresses authentication, and includes provisions for mutual authentication between the ISIM on the UE and the S-CSCF (so that both ends of the connection have assurance that they are communicating with the right party). The HSS is responsible for key generation and the initiation of authorization challenges.

Security Association 2 addresses security of the link between the UE and the P-CSCF to protect communications between them.

While the UE initiates contact by establishing a connection first to the P-CSCF, it is the home S-CSCF and the HSS of the UE that are ultimately responsible for authentication. This model is the same regardless of whether the subscriber is connecting to the IMS network via a P-CSCF on the home IMS or is roaming and connecting to another IMS network's P-CSCF.

In the event of a roaming scenario (Scenario 1 from Part One of this paper), where the UE is connecting to a P-CSCF that belongs to an IMS domain that is different than its home domain, the P-CSCF submits the UE authentication request to the I-CSCF for forwarding to the appropriate home IMS domain. The UE informs the P-CSCF of its home IMS domain information as part of the registration request. [4] The P-CSCF will use this information to perform a lookup to locate and contact the appropriate I-CSCF for the subscriber's home IMS network.

The I-CSCF then queries the HSS (Home Subscriber Server) to determine to which S-CSCF to send the request. The S-CSCF, recognizing that the UE is not authenticated, sends a challenge back to the UE and begins the process of establishing a secured channel from UE to P-CSCF. Once that channel has been established, a secured SIP registration can be issued and processed by the S-CSCF for the session request to proceed. This process is known as IMS AKA (Authentication and Key Agreement). The S-CSCF retrieves user profiles from the HSS via the Diameter protocol and does not maintain local records of users.

The AKA process provides the ability to confirm the integrity of the traffic as a means to ensure that the traffic between the UE and the P-CSCF has not been tampered with.

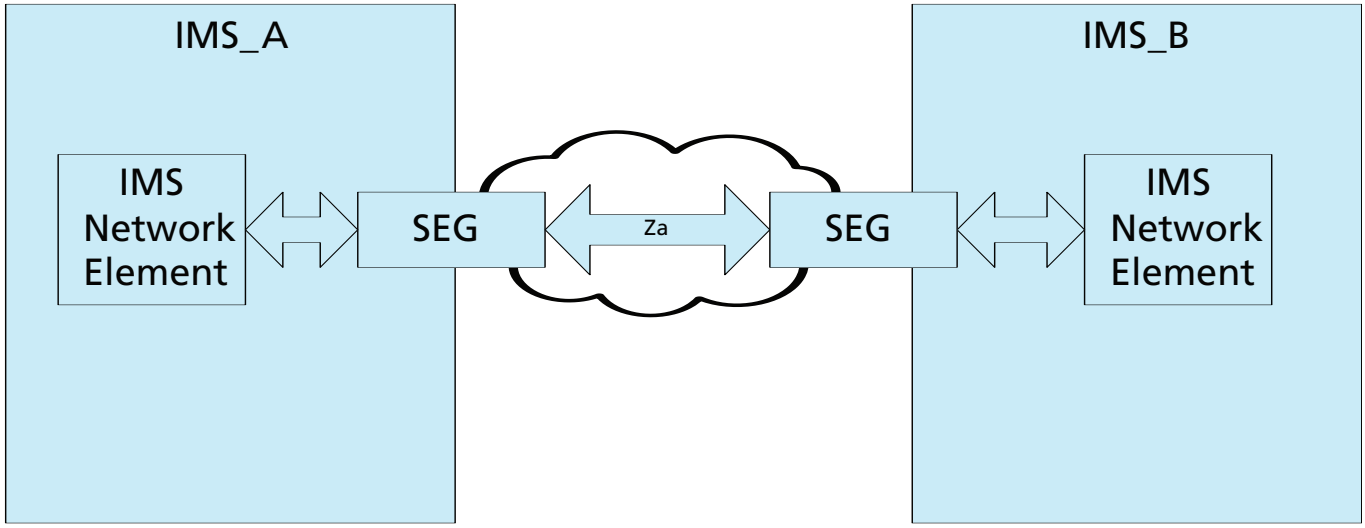
Another activity that occurs during the establishment of the security association is the determination of the type of encryption to be utilized to secure communications between the UE and the P-CSCF (either DES-EDE3-CBC, AEC-CBC, or no encryption).

Security Association 4 Overview – Visited P-CSCF to home I-CSCF & S-CSCF

Security Association 4 identifies requirements for communication security in an IMS roaming subscriber scenario (Scenario 1 from Part One of this paper).

The standards indicate that any IMS control plane traffic that travels between elements from two different security domains (in this case, two IMS networks, each owned by a different carrier) must be routed through Security Gateways (SEGs) over the Za interface. The Za interface provides for mandatory authentication & integrity protection and a recommendation for encryption (via a tunneled IPSec ESP connection) [2]. Negotiation and establishment of the connection is performed by IKE. These connections can be established on a long term basis or on an as-needed basis. Details of the connection would typically be determined through the development of a roaming agreement between the two IMS network carriers. The architecture for the SEGs and the Za interface is shown in figure 2.

FIGURE 2 – SEG Architecture



Security Association 6 & 7 Overview – IMS Network to IMS Network

Security Association 6 provides for communication security between an HSS within the home IMS network and an Application Server (AS) located outside the home IMS network. Security Association 7 defines security between nodes located in the home IMS network and nodes located outside the home network.

The primary requirements specified for SAs 6&7 are identical to SA4- – that the nodes should communicate with one another through a SEG that supports IPSec, and that the associations between the networks should be negotiated using IPSec IKE. The key assumption is that nodes outside the home IMS network are secure and trustworthy.

The implication of this assumption is that there must be some level of trust between the IMS network operators – each operator must trust that the other operator has a secure IMS implementation. One way to implement this would be to limit the number of interconnection points to a minimal set of trusted operators. Alternatively, an operator would need to take precautions to limit the types of traffic that would be permitted to pass to or from other connected IMS networks. Vendors of session border controllers have positioned their products as a means to provide this type of access control.*

* One other significant note is that the specifications focus primarily on scenarios where the home IMS network is communicating with an external application server, with minimal references to other types of connections. 3 There are no specific references to IMS peering within these specifications.)

Session Border Controllers

Session border controllers (SBCs) can play a key role in the IMS infrastructure to secure the areas where the IMS needs to connect to potentially un-secured networks.

One method of implementing an SBC is to configure it to act as a proxy for SIP sessions between UEs and IMS network elements. In this type of configuration, the SBC can provide Network Address Translation (NAT) functionality, so that the carrier can control the visibility of network addresses on either side of the SBC. For example, the carrier could utilize private, reserved IP addresses for the IMS network elements by utilizing the SBC to provide NAT services between the private-IP-addressed core IMS elements and the public-IP-addressed UEs. This same function can also be done in reverse, where the carrier might choose to utilize private IP addresses on the access network side for the UEs.

SBCs can also serve as an IMS application layer gateway (ALG). When it performs ALG functions, the SBC acts in the role of a SIP B2BUA (back-to-back user agent) as defined in the 3GPP IMS specifications [5], This enables IMS elements on either side of the SBC to think that they are talking directly to one another, when in reality they have each established sessions only to the SBC itself. One possible function for an ALG is to provide interworking between networks that are using different versions of IP – for example, an element on one network may be utilizing IPV4, while the network for the destination element is running IPv6.

SBCs typically provide some form of basic access control lists (ACL), to prevent unauthorized users or traffic from/to unauthorized ports. Something else an SBC does that is critical and distinguishes itself from other ALGs is the logical analysis of call flows – that is to say that the SBC has the ability to compare traffic flows against normal traffic patterns. If an abnormal traffic pattern is detected, such as an excessive number of concurrent sessions from a single UE or a large number of repeated call attempts, the SBC will block that traffic and refrain from forwarding on to the secured network. Behaviors such as the repeated dialing of a new number every few seconds while incrementing the dialed number by one on each successive attempt would be suspect. Another example would be a single UE attempting to make 100 new call attempts at once; which could be indicative of an attempt to launch a Denial of Service (DoS) or Distributed Denial of Service (DDos) attack.

In addition to providing security on the VoIP network, SBCs can also act as a security mechanism between the IP network and the PSTN. In some architectures, UE traffic is routed to the SBC to then be routed out to the PSTN through a gateway.

As SBCs have evolved, they have become more specialized to focus on protection for certain areas of a network. This is especially true with regard to SBCs within an IMS network. One type of SBC implementation can be classified as an access SBC (A-SBC), placed at the edge of the access network and the core network – the place where users first gain access to the IMS core. In this mode, the SBC can act as an access border gateway function (A-BGF) to provide access controls, as well as network address translation (NAT)

Another function of an SBC can be to act as a security enforcement point between peer IMS networks. When used for this application, an SBC is referred to as an Interconnect SBC (I-SBC). Currently, most SBC products provide border control functions for both the signaling and the bearer traffic. These functions may be distributed in the future per the specifications within 3GPP version 7, whereby the border control for signaling would be provided by an I-BCF and control of the bearer traffic would be performed by an I-BGF.

An Interconnect SBC can act as a Topology Hiding Interconnect Gateway (THIG), as specified by 3GPP release 6 [5] . When acting as a THIG, the SBC prevents details about the core IMS network and elements (such as host names or IP addresses) from being transmitted to other, less secure networks. A network element that provides the THIG function will inspect the SIP traffic, and will re-write sensitive information from the headers that can reveal topology information, such as the Via, Route, Record-Route, and Service-Route headers [6] Other common SBC functions include providing some level of QoS control and the ability to defend against common types of Denial of Service (DoS) attacks.

The I-SBC will typically be located in the network architecture between the I-CSCF and the external network connection. As the technology evolves, SBCs, (or devices like them) will act in the roles of the Security Gateway (SEG), and/or as the I-BCF or I-BGF. Some vendors may choose to implement specific network elements to perform one or all of these roles, or they may build functionality (such as SEG capability) into existing elements.

The facilities described in this section provide the basic security functionality required for authentication of UEs and for the protection of the core IMS network. The next section will illustrate how these facilities work together in the context of an interconnected multiple IMS architecture.

Detailed Call Flow for Interconnect Scenario & Identification of Potential Vulnerabilities

With a conceptual groundwork laid for the IMS interconnect models and the basic security provisions contained within the IMS standards, the next step is to analyze an IMS session flow to illustrate how the various elements (IMS functions, security associations, and interconnect models) will interact.

As the various connections between elements are described, any notable security considerations will be identified with a consideration of traditional security threats such as confidentiality, integrity, authenticity, and denial of service.

Note: The majority of the security considerations identified in this section pertain to the SIP session layer (layer 5). There may be additional security considerations that apply to the lower layers (such as any issues related to the protection of layer 3 routing information) that are not addressed by this paper.

This example is based upon interconnect scenario 2 (peering between two IMS networks) identified in Part One of this paper. In scenario 2, a subscriber on IMS network A (SUB_A1 on IMS_A) attempts to establish a session with a subscriber on IMS network B (SUB_B1 on IMS_B)

Subscriber A has already powered up their UE, the UE has received the P-CSCF address as part of the DHCP address assignment process. In this scenario, SUB_A registers from within its network, so the P-CSCF is part of the IMS_A network. The UE for SUB_A utilizes SAs 1 and 2 for authentication with the S-CSCF and HSS, via the P-CSCF and the I_CSCF (SA1), as well as to establish security on the link between the UE and the P-CSCF (SA2).

Next, SUB_A initiates a call to SUB_B, using either a TEL URI or a SIP address. The request is transferred through the P-CSCF and I-CSCF to the S_CSCF. The S-CSCF examines the INVITE message to determine if the destination is local to IMS_A. Since the destination belongs to a subscriber on different IMS network (IMS_B), the request needs to be forwarded to IMS_B.

The mechanisms for how the invite is forwarded to IMS_B, and how the traffic is passed between the two IMS networks are clear – but the methods by which to implement the connections between the networks are critically important with respect to the level(s) of security that can be ensured. Following is a step-by-step detailed analysis of each of these activities based on Section 5.5.1 of 3GPP TS 23.228, and Section 5.4 of TS 24.229

1. The S-SCSF in IMS_A determines that SUB_B is a subscriber on IMS_B (either by analyzing the domain name within SIP URI (SUB_B@IMS_B) or by performing an ENUM lookup to by analyzing the Naming Authority Pointer (NAPTR) record to resolve a TEL URI into the SIP address for SUB_B. If the ENUM does not respond with a valid SIP address, the S-CSCF will forward the request to the BGCF to be sent out to the PSTN.
   a. Security Note – The assumption within this step is that the S-CSCF is utilizing a trusted ENUM server. This will require that the ENUM server is either controlled by a trusted party or that sufficient mechanisms are in place to ensure the accuracy and integrity of the data for domains IMS_A and IMS_B. The risks of using an un-secure ENUM/DNS infrastructure include things like potential for denial-of-service attacks and introduction of incorrect data into the DNS records to intercept session invites. Therefore, access to a secure ENUM/DNS infrastructure becomes the first requirement for secure interconnect.
2. The S-CSCF analyzes the destination address, and determines that the address refers to a location that is not served by IMS_A. Using the domain name data from the SIP URI, the S-CSCF determines the address for the pre-published entry point of IMS_B through a DNS lookup.. (Note that this entry point could be an address for an element on a transit network that would provide the routing between the IMS networks.)
   a. Security Note – Again, the ability to resolve accurate, secure information from the DNS infrastructure is a requirement for this step. This reinforces the need for a trusted DNS.
3. The S-CSCF sends the INVITE to the I-CSCF for egress from IMS_A. This element may be providing THIG functionality, and it may be combined with the additional SEG functionality to provide integrity and encryption. Since this is a case where traffic is traveling between two different IMS networks, Security Association 7 should apply (FOOTNOTE: Currently there are limited options for vendor implementations of a SEG per TS 33.210, so carriers are evaluating alternative means for providing similar functionality).
   a. Security note – If the IMS_A architecture does not include a SEG, the traffic exiting IMS_A will be sent unsecurely & unencrypted – thereby making it a requirement that security for the links between IMS_A and other IMS networks be provided by other means. This could be accomplished through the use of a lower-layer secure VPN connection between the carriers, through dedicated point-to-point links, or by providing encryption through routing devices or through session border controllers. This requirement limits the ability for carriers to establish "ad hoc" connections to other carriers, because it would require all carriers to use the same encryption mechanism.
4. The I-CSCF in IMS_A forwards the INVITE message to the I-CSCF of IMS_B across the interconnected IP network.
   a. Security note – the minimum required connectivity between the networks is an infrastructure that is capable of delivering the layer 5 SIP messages over IP (layer 3). There are many reasons why a public network such as the Internet would meet these criteria, but would be undesirable from a security perspective. The issue of encryption was mentioned in the previous step, but there are additional considerations with respect to the inability to guarantee performance levels, reachability, and Quality of Service (QoS) over an Internet link. Carriers will likely employ a similar model to what they are providing for other types of interconnectivity with other carriers, such as dedicated point-to-point connections or secured private networks.

b. Another important point to make here is that the traffic will likely flow through an SBC or other type of SEG as the traffic flows between the networks.

5. The I-CSCF in IMS_B will query the HSS in IMS_B to determine the appropriate S-CSCF for SUB_B, and will forward the request to that S-CSCF.
6. The S-CSCF in IMS_B will invoke the appropriate service logic and forward the INVITE to the P-CSCF and on to SUB_B

Recap of the Key Requirements

From the walkthrough, it is clear that there are two primary requirements to ensure adequate security between the interconnected networks.

1. Some level of shared DNS/ENUM infrastructure is required between any peering partners. Access to this infrastructure must be secured by some means to reduce the possibility of attacks. This precludes the use of the public DNS/ENUM infrastructure as the mechanism for resolution
2. In order to protect the signaling traffic between peer IMS domains, appropriate mechanisms must be established to ensure the integrity and privacy of the traffic. This can be accomplished per the technical standards through the implementation of a Security Gateway (SEG), or through other elements such as session border controllers that have the appropriate capabilities. Alternatively, carriers can establish private, dedicated links to peering partners at the network layer, but even then, each carrier will be responsible to protect their network through the use of a firewall, or other security mechanisms.
3. Both #1 and #2 preclude the possibility for establishing "ad hoc" connections between carriers, so the number of potential IMS peering partners is limited to the number of partners with which a carrier wishes to establish a formal peering agreement. One potential alternative would be for the establishment of a trusted third-party carrier to act as a hub/transit network between multiple IMS domains.

Conclusion – Looking Forward

The standards related to IMS interconnect and peering are continuing to evolve, as evidenced by the introduction of interconnect-specific functions within 3GPP Release 7 (I-BCF, I-BGF). These elements provide a separation between control of signaling activities (I-BCF) and control of bearer traffic (I-BGF) to provide better scalability.

At the same time, groups like the recently created IETF Session PEERing for Multimedia INTernetworking (SPEERMINT) group are addressing many of the complex issues associated peering, including definition of minimum peering requirements [7], identification of call routing procedures, and definition of peering federations (groups of providers that agree to transfer calls between each other and agree upon rules that govern those calls, such as security provisions and definition of how settlements will occur).[8] SPEERMINT is also focusing on some mechanisms that will enable ad hoc peering between providers that do not already have a peering agreement in place.

As carriers complete their initial IMS trials and begin to commercially deploy IMS-based services to their subscribers, the business benefits for IMS interconnect and peering will drive carriers to explore how best to provide connectivity to other carriers' subscribers.

By implementing this connectivity according to the security provisions in the existing standards, and by focusing on the areas with potential vulnerabilities, such as utilizing a secure DNS/ENUM architecture and by securing the traffic flows between one another, carriers can benefit both their subscribers and their own bottom line in a more secure way.

References

[1] 3rd Generation Partnership project. *Access Security for IP-Based Services*, 3GPP TS 33.203, October 2006

[2] 3rd Generation Partnership project. *3G Security, Network Domain Security, IP Security*, 3GPP TS 33.210, September 2006

[3] 3rd Generation Partnership project 2. *IMS Security Framework, Network*, 3GPP2 S.S0085-B, December 2005

[4] 3rd Generation Partnership project. Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), 3GPP TS 24.228, October 2006

[5] 3rd Generation Partnership Project. *IP Multimedia Subsystem (IMS) Stage 2, Release* 6, TS 23.228 V6.14.0, June 2006

[6] 3rd Generation Partnership Project. IP Multimedia Call Control Protocol Based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3, 3GPP TS 24.229, October 2006

[7] IETF SPEERMINT Working Group. SPEERMINT Requirements fo SIP-based VoIP Interconnection, draft-ietf-speermint-requirements-01.txt, October 2006

[8] IETF SPEERMINT Working Group. SPEERMINT Terminology, draft-ietf-speermint-terminology-06.txt, September 2006

List of Acronyms

3GPP	3rd Generation Partnership Project
A-BGF	Access Border Gateway Function
AGCF	Access Gateway Control Function
AKA	Authentication and Key Agreement
ALG	Application Layer Gateway
AS	Application Server
A-SBC	Access Session Border Controller
B2BUA	Back to Back User Agent
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
ENUM	tElephone NUmber Mapping
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
I-BCF	Interworking Border Control Function
I-BGF	Interworking Border Gateway Function
I-CSCF	Interrogating Call Session Control Function
IPSec IKE	IP Security Internet Key Exchange
IMS	IP Multimedia Subsystem
IP	Internet Protocol
I-SBC	Interconnect Session Border Controller
ISIM	IMS Subscriber Identification Module
ISP	Internet Service Provider
IWF	Inter Working Function
LAG	Line Access Gateway
LAN	Local Area Network
MGCF	Media Gateway Control Function
MMS	Multimedia Message Service
NAP	Network Access Point
NAT	Network Address Translation
P-CSCF	Proxy Call Session Control Function
PDG	Packet Data Gateway
PES	PSTN Emulation System
PSTN	Public Switched Telephone Network
SA	Security Association
SBC	Session Border Controller
SEG	Security Gateway
SIP	Session Initiation Protocol
SMS	Short Message Service
SP	Service Provider
THIG	Topology Hiding Internetworking Gateway
TISPAN	Telecommunications and Internet Converged Services and Protocols for Advanced Networking
UE	User Equipment
URI	Uniform Resource Identifier
VoIP	Voice over IP
VPN	Virtual Private Network

Acknowledgements

Thanks to the many who provided input, review, and comments for this paper. Special thanks to Jason Boswell for his early contributions to the development of the paper. Thanks also to Jean-Philippe Joseph, Jack Barnett, and Basheer Tannu for their feedback.

About the Author

Morgan Stern
Principal Consultant, Global Convergence Center of Excellence
Alcatel-Lucent Services

Morgan Stern provides guidance to service providers in the development and implementation of network evolution initiatives. In his role, he draws upon experience gained during more than 15 years in the telecom and IT industries assisting clients in areas such as network optimization, VoIP migration, IMS architecture design, IT integration, and network convergence. He is the author of three books and a variety of articles and papers on IP network services, network security, and directory services.

www.alcatel-lucent.com