



# IMS AAA Architecture: The Diameter Advantage

White Paper

September 2009

## **ABSTRACT**

IMS standard bodies have chosen the Diameter protocol to enable AAA (Authentication, Authorization and Accounting) capabilities. As the AAA is a key functionality for managing a communication infrastructure, protocols involved have to be secure, to make the scalability easier, to be flexible and to be able to evolve easily and quickly.

This paper will show that the Diameter protocol delivers the combination of scalability, flexibility and security required for the delivery of multimedia services over IP. IMS architectures and servers are used to show the Diameter capabilities. And a number of issues, such as the compatibility of multiple Diameter releases used in the same network, will be presented.

## 1. THE DIAMETER PROTOCOL

Diameter is a signaling protocol created to resolve the main issues that the RADIUS (Remote Access Dial-In User Service) protocol left open. Specified by IETF, this protocol has been adopted by 3GPP (3<sup>rd</sup> Generation Partnership Project) and 3GPP2 standardization bodies for AAA in IMS mobile systems and networks. It is also the AAA protocol selected by TISPAN (Telecoms & Internet converged Services & Protocols for Advanced Networks), the ETSI (European Telecommunication Standards Institute) committee in charge of FMC (Fix Mobile Convergence) standardization.

### 1.1. WHAT IS DIAMETER?

The Diameter protocol consists of a base protocol, a transport profile defined in [RFC3539] and applications (also called extension of the base protocol). The base protocol brings the common functionalities supported by all the services like mechanism for message delivery, error notification, session handling and capabilities negotiation. As a result, the base protocol must be supported by all applications. The transport profile defines the main properties and recommendations of the transport layer for AAA systems (the failover mechanism and related state machines). The Diameter protocol uses Transmission Control Protocol (TCP) or Stream Control Transmission protocol (SCTP) for transport. Various Diameter applications are defined for extending the base protocol: this capacity is the major concept of the protocol. Depending on the final usage of the service, a Diameter application can be defined to add semantic information and, as a result, to specialize the base protocol. For example, the Diameter Credit Control Application (CCA) is defined in the [RFC4006] document to add all the information necessary for the on line charging services.

### 1.2. DIAMETER PROTOCOL MAIN CONCEPTS

#### 1.2.1. Message structure and properties

The Diameter protocol is a binary signaling protocol. The Diameter messages are 32 bits padded to simplify the processing. The base protocol defines the format of the commands (or messages) which is composed by a header and the body defined by a set of the Attribute-Value Pairs (AVPs).

The Attribute-Value Pairs are a method for representing the relevant data or AAA specific information. AVPs are encoded as TLV (Type Length Value) with an optional possibility to add vendor specific information (coded within a vendor identifier). A set of commands, AVPs and AVPs values is defined in the base protocol or in a Diameter application document. Applications can extend the protocol by defining new commands, AVPs values and AVPs and append them to the commands. Like for the AVPs, applications can define vendor specific commands.

#### 1.2.2. Network elements and architecture

Different types of Diameter node are defined:

- A Diameter client is at the edge of the network.
- A Diameter server handles the AAA Diameter requests for a specific realm. The realm is an administrative domain.

The protocol also defines different types of agent for simplifying the network architectures. A Diameter agent can be a relay, a proxy, a redirect or a translation agent:

- A relay agent is used for routing the messages to the Diameter server.
- A proxy agent acts like a relay, but can modify the messages and generally implements policy enforcement and an admission control mechanism.
- A redirect agent is only used for indicating where the sending peer has to forward its request.
- A translation agent is used to provide a translation between Diameter and other protocols.

### 1.2.3. Peer-to-peer infrastructure

The different Diameter nodes are interconnected in a peer-to-peer infrastructure. A Diameter node should be connected to two peers per realm: a primary and a secondary which is used in case of failure of the primary one. The peer-to-peer infrastructure participates to the robustness of the deployment of the protocol. A mechanism for dynamic peer discovery is also defined.

### 1.2.4. Capabilities exchange phase

The connection between two peers is established after a capabilities exchange phase. During this phase, the compatibility between the Diameter applications supported by the peers is checked. If an incompatibility is detected, the communication is not established. As a result, two connected nodes support compatible applications.

### 1.2.5. Realm based Routing

The messages are routed using a routing table which is called Realm-Based Routing table. It contains the route information of every realms and applications supported locally or externally inside a Diameter node. This table can be updated during the capabilities exchange phase. Diameter infrastructure allows static but also dynamic routing. In other words, the Realm based routing mechanism is the concept, extended from RADIUS, which enables the control of the routing for the Diameter messages used for a service execution. Better than a simple IP routing, it is a representation of the deployment of connected Diameter nodes.

### 1.2.6. Failover mechanism of Diameter

The Diameter protocol uses application layer acknowledgements and defines the failover algorithm and the associated state machine. In fact, the protocol follows the AAA Transport profile defined in [RFC3539]. Peers follow a state machine with a device watchdog mechanism for immediately detecting a transport failure and handle the state of the connection. If a transport failure is detected with a peer, the messages pending are marked (with the T flag) and forwarded to another node (the secondary). This failover mechanism preserves the transaction level: the requests forwarded are those who have not been answered.

### 1.2.7. Security

Two different levels of security can be enabled with the Diameter protocol: hop by hop security and also end to end security. The first one is used to provide security across a

transport connection using IP security (IPsec) or the Transport Secure Layer (TLS) and the second one is used to have an entire safe communication path between two diameter nodes. Diameter is designed to simplify the handling of the security: this is an important property for AAA.

### 1.3. DIAMETER USAGE INSIDE IMS

IMS is a standardized framework for telecom operators to provide mobile and fixed multimedia services in an all IP environment. It was created to make network management easier and to provide better interoperability, roaming between networks and also network convergence.

#### 1.3.1. IMS architecture and functionalities

The architecture of the IMS framework is based on the definition of functions and standardized interfaces. It is done by 3GPP. There are different releases corresponding on the different phases of development.

The latest IMS architecture is described in release 8.

The IMS architecture defines three layers:

- The application plane contains applications and content servers that implement the value added services for users. This layer is interfaced with the control layer to enable combinations of the applications that run on the application servers.
- The control plane is used for call and session control, provisioning and charging. The main functions of this plane are: the HSS (Home Subscriber System), the CSCF (Call Session Control Function), the BGCF (Border Gateway Control Function) and the MRFC (Media Resource Function Controller).
- The transport plane consists of Media Gateways, routers and switches for the backbone and access networks, both fixed and mobile.

The main signaling protocols used inside IMS are SIP for the management of user multimedia sessions and Diameter for AAA capabilities and provisioning. Diameter takes an important role in the core signaling functionalities of the IMS.

#### 1.3.2. Diameter usage and localization

All the interfaces of the IMS dealing with charging, Authentication, user profile management, checking right to access network resources, are based on the Diameter protocol. Most of the time, these interfaces define need to a specific Diameter application in order to carry on the ad-hoc control and data exchanges. Generally, the vendor identifier used for these applications is 3GPP (for the extended part); the application identifier is a 3GPP one (except for the accounting).

The following table is not exhaustive but gives the main reference points where a Diameter application is defined:

Name	Location inside IMS	Purpose
Cx, Dx	HSS, CSCF	Authentication and Authorization
Gq	AF, PDF	Policy Control
Gx	GGSN, PCRF	Policy & Charging Control Accounting, charging rules provisioning
Gy	GGSN, OCF	Accounting, on-line charging (Ro equivalent)
MM10	MMS relay/server, MSCF	Multimedia Messaging Service
Pr	PNA, AAA server	WLAN related interface for presence
Re	OCS, RF	
Rf	CSCF, BGCF, MRFC, MGCF, AS	Accounting, off-line charging
Ro	MRFC, AS	Accounting, on-line charging (See also Gy)
Rx	CRF, AF (P-CSCF)	Policy and Charging Control
Sh, Dh	AS, HSS/SLF	User profile management
Wa, Wd, Wg, Wm, Wx, Dw	WLAN AN/AAA Proxy/WGA/PDG/HSS, SLF/AAA proxy/server	WLAN related interface
Zn, Zh, Dz	NAF/HSS/SLF, BSF	Authentication
S6a, S6d	MME/S4-GGSN, HSS	Authentication
S6b	3GPP AAA Server/Proxy and PDN GW	Authentication
S9	PCRF in the HPLMN (H PCRF) and PCRF in the VPLMN (V PCRF)	Policy and Charging
S13	MME and EIR	Query subscriber authentication information
Gxa, Gxb, Gxc	PCRF/PDG, BBERF/vPCRF	Exchange of QoS information between functions of PCC architecture
SWa, SWd	un-trusted non-3GPP IP access/3GPP AAA Proxy 3GPP AAA Server/Proxy	Authentication for interworking with non 3GPP networks.
SWn, SWm	Un-trusted Non-3GPP IP Access/3GPP AAA Server, ePDG	Authentication for interworking with non 3GPP networks.
SWx	3GPP AAA Server and the HSS	
H2	3GPP AAA Server, HA	Authentication for interworking with non 3GPP networks.

The number of interfaces using Diameter is important and changes depending on the 3GPP release considered. From release 5 to the release 8, the number of interfaces using Diameter is growing: New reference points are defined using Diameter or some protocol of already existing reference points are replaced by Diameter. This increase is mainly due to

the adding of new functions or components (QoS or Policy), or the definition of gateway between 3GPP system components and non-3GPP systems.

For example, since the release 6, COPS (Common Open Policy Service) protocol used in the Go interface is replaced by Diameter used as an AAA protocol that can deliver policy control in the Gx interface.

The charging interfaces used by 3GPP (Ro, Rf, Gx ...) are just extensions of the [RFC3588] for off-line charging and [RFC4006] for on-line charging. The state machines used are directly a sub set of the ones defined in the RFCs.

## 2. ADVANTAGES OF DIAMETER PROTOCOL

After this brief description of the protocol and the usage inside IMS, some properties are pointed out in this chapter in order to show the advantages of Diameter at different levels: functional, service delivery and also network deployment. When it is possible, advantages will be illustrated inside the IMS.

### 2.1. EXTENSIBILITY AND FLEXIBILITY

Different RFC documents (RFC3588, RFC4004, RFC4005, RFC4006 ...) define Diameter applications. The Diameter protocol is designed to be extensible: there two are different possibilities depending on the usage of the protocol. All of them are used by 3GPP inside IMS.

- If an existing application suit to the AAA problem but some information has to be added: new AVP values or new AVPs can be created to be used in the already existing command of a specified Diameter application. The Diameter AVP representation can contain vendor specific information. This case can be illustrated by the 3GPP Ro application which uses a RFC4006 Credit Control Diameter application with 3GPP vendor specific AVPs and 3GPP AVP values.
- If there is no existing application that suit to the AAA problem, a new authentication/authorization or accounting application can be created by creating a new application identifier (vendor specific) and probably new commands. For sure the usage of AVPs and AVP values of already existing application or base protocol is possible (and recommended by the RFC3588), but new AVPs can also be created. This case can be illustrated by the 3GPP Sh Diameter application which defines a new application for user profile management.

NEPs (Network Elements Providers) can easily take advantages of these two mechanisms to exchange specific data and maintain the compatibility at the same time.

### 2.2. SECURITY

As the protocol carries authentication, authorization and accounting information, the security is a very important feature especially when using intermediate node (for roaming for example) during a call.

The hop by hop security mechanisms of Diameter enables both intra-domain (with the usage of IP sec) and inter-domain (with the usage of TLS) AAA deployments. TLS or IPSec are used to eliminate untrusted Diameter agents present in the path between two communicating Diameter nodes.

When IPsec transport mode is used, encryption and authentication algorithms are used to provide per-packet authentication and confidentiality. Peer authentication, key management and negotiation of IPsec security associations are done through Internet Key Exchange (IKE).

Concerning TLS mechanisms, it is adapted to the Diameter protocol. The two communicating peers indicate the support for TLS to each other through the capabilities negotiation mechanism. The peers need to start the TLS handshake just after the capability exchange phase.

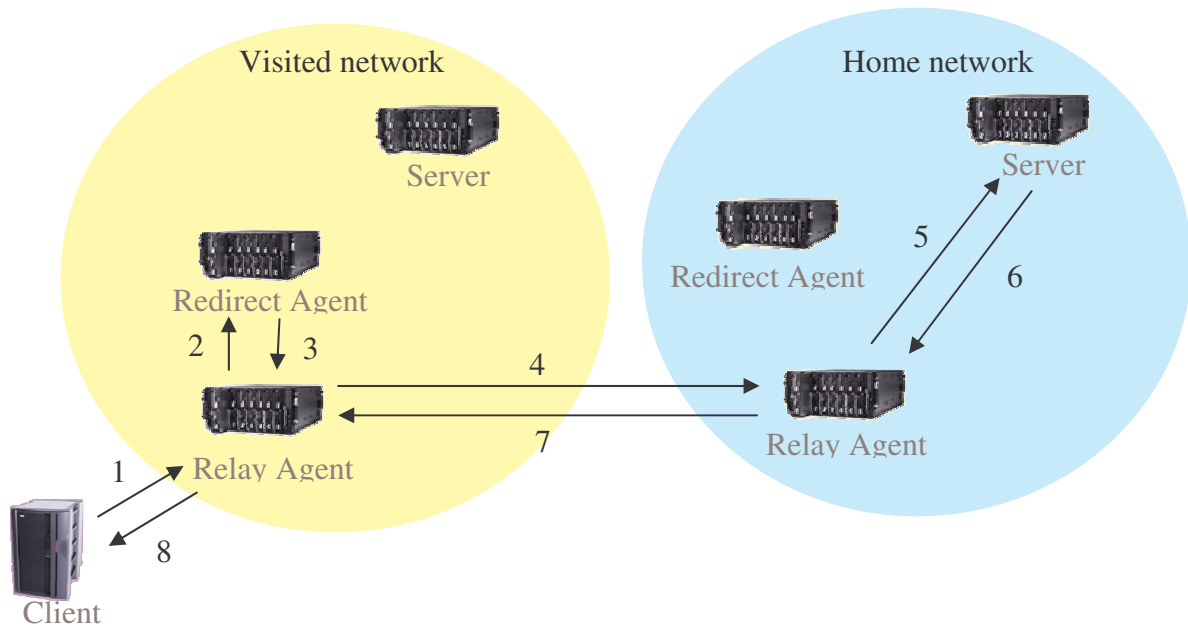
The end to end security mechanisms of Diameter are used to protect the integrity and/or the confidentiality of sensitive AVPs through intermediate untrusted nodes.

## 2.3. INTER-DOMAIN COOPERATION

Diameter is especially designed to handle issues that arise when multiple realms are invoked. An example of multiple realms is the roaming. The roaming is the situation where the user is connected to a network that is not the network of its own internet service provider. In this case the user is located at a different realm as the one he belongs to, and the realm which the user is visiting has to verify authentication and authorization of the user at his own realm.

As explained previously, the realm based routing mechanism and the definition and usage of different agent (especially relay and redirect) are elements that can be used to provide AAA with inter-domain cooperation. Concerning the security, Diameter trust is based on a pre-configured set of roaming Certificate Authorities (CAs) but requires Public Key Infrastructure (PKI) with the CAs.

A roaming situation can be easily handled with a Diameter redirect agent located in the visited domain. A Diameter server that receives a request concerning a user from a foreign domain can forward the request to a Diameter redirect agent to obtain the information concerning the node that can treat the request. This mechanism involves that Diameter nodes are registered in a sort of roaming federation. But the cooperation can be resolved differently if the visited network is in capacity of executing the service required by the user. The following schema explain the diameter elements what can be deployed to handle a roaming situation and the order of the exchanges of messages.



*Example of roaming handling architecture with Diameter nodes*

For IMS, an inter-domain cooperation corresponds to an inter-operator cooperation (between an operator, a MVNO or a third party content provider) for doing roaming or for providing other services. An interface like Wd (see section [1.3.2]) is defined for this kind of purpose for interworking between 3GPP systems and WLAN. This interface can be used in a roaming case when an operator offers a WLAN access, to propagate: authentication information, authorized services information (IP filtering...) or QoS profile.

## 2.4. RELIABILITY

The reliability of the usage of the Diameter protocol is ensured by multiple mechanisms.

First of all, the transport used by the protocol is a connection-oriented one: TCP or SCTP. It involves the support of flow control and congestion avoidance mechanism. The selection of this kind of transport is done to follow the RFC 3539 document which defines the transport profile for AAA. If the two transport are supported: SCTP is firstly preferred to TCP. Some guidelines are also given to take advantage of the usage of SCTP: Even the capability exchange phase is adapted to SCTP special features like the support of multiple IP.

Second, the failover mechanism defined in the Diameter protocol is also an element of reliability. It involves that a queue of pending messages is maintained by every Diameter node until a transaction (request/answer) is not entirely performed. When a peer detects a transport failure, the pending messages are marked (to facilitate the process of duplicate messages) and forwarded to another node. The Diameter protocol defines its own mechanism of retransmission and prevents from the treatment of duplicated messages. The failover mechanism is based on the usage of a primary peer and a secondary peer in case of failure. As a result, it can easily be mapped or used inside a redundant high availability system.

An additional mechanism is also supported for the treatment of disconnection of the peers. If a peer is disconnected without a dedicated base protocol message (Disconnect-Peer-Request), the remote node will periodically attempt to reconnect (depending on the properties of its routing table).

## 2.5. RADIUS COMPATIBILITY AND REPLACEMENT

The first RADIUS specification was proposed to be a standard in 1997. Many articles extend its ability and commercial products adopt RADIUS to provide AAA model. However, network entities have increased in complexity; deficiencies in the RADIUS protocol have been identified. In some researches and experiments, RADIUS protocol is already validated that it has many security weaknesses. The Diameter protocol is designed to resolve some issues of the RADIUS protocol (security, transport, failure detection, size of the data).

Diameter does not share a common format of the commands with RADIUS. Command codes and AVP codes are shared between the two protocols. As a result, a translation agent is required for passing information from one protocol to the other one. More over, the current important deployment of RADIUS protocol is a reason for the coexistence of these two protocols.

An illustration of the usage of a Diameter translation agent inside the IMS architecture can be given with the Wd reference point example (see section [1.3.2]). This reference point is defined between the 3GPP AAA proxy and the 3GPP AAA server. Depending on the WLAN AN (Access Network) characteristics, the Wd reference point uses RADIUS or Diameter. As the AAA proxy is the only network element in contact with the WLAN, a RADIUS/Diameter translation agent is required and defined by 3GPP inside this element.

## 3. DIAMETER IN OPERATION

As Diameter protocol is more and more used interoperability events are needed as a part of the integration of an implementation of the protocol for a given functionality inside IMS. This chapter will browse the most common issues encountered during Diameter interoperability events. Two levels will be considered:

- The peer connection management level and then
- The Diameter application data exchange level.

As the extension of the protocol is very simple, the capability exchange phase is very important to be sure that two peers will be able to communicate and the services on top of them will understand the information needed depending on the role of the node. As a result, the vendor specific information (supported vendor identifier) is exchanged.

### 3.1. PEER CONNECTION MANAGEMENT LEVEL

The coherence of the information exchanged during the initial capabilities exchange phase is very important. The capabilities exchange is not clearly specified in the [RFC3588] but just deducted from the state machines. Depending on the Diameter node element, the list of supported vendor identifiers given in the messages will influence the establishment of the communication. The support of vendors is not necessary present inside intermediary nodes: the main interoperability problems that occur are due to a lack of provisioning information in these intermediary nodes.

### 3.2. EXCHANGE OF COHERENT APPLICATION DATA

#### 3.2.1. Application version and implications to IMS

An important problem encountered particularly inside IMS, is the problem of the version of a Diameter application. When the applications are modified from one release to another one,

the set of AVP is changed, but generally the application id is not modified by 3GPP. As the information of the release is not present in the message or has to be guessed, some interoperability problem can occur. The base protocol itself has its own mechanism for the versioning, but it is not the case of a Diameter application. There are two possibilities for doing that: the first one is to have a different application identifier and the second one is to use a specific AVP. There is no specific AVP normalized.

### 3.2.2. Application data handling with the mandatory flag

The problem of the usage of the M-bit is one issue that can be encountered. This M-bit (for Mandatory bit) is a flag used inside an AVP. The flags are used to cause a particular behavior to the receiver. According to [RFC3588], this flag has to be set for an AVP inside a command of an application, to indicate that this AVP must be supported. As the connection is considered as already established, the application is supported by the receiver. As a result, all the receivers that have published the same application must understand this AVP. That is the reason why the M-bit does not influence relay or redirect node, but only client, server and other agents. In these last three cases, a message received with an M-bit set to an AVP not understood has to be rejected. A lot of problem encountered are due to inappropriate setting of this flag. Generally, there is confusion between the ABNF defining the set of AVPs used in a Diameter command for a particular Diameter application and the setting of the M-bit of an AVP for this same application.

### 3.2.3. Result code interpretation and error handling

When a Diameter node receive an answer, the Result-Code AVP and the E-bit (Error Bit flag) are used to interpret the transaction. The result code value follows a hierarchy defined by IANA. But, for a particular vendor-specific request, the Experimental-Result grouped AVP containing Experimental-Result-Code AVPs has to be used for vendor specific result code. An answer must contain a Result-Code or an Experimental-Result: this is an exception of the vendor specific general mechanism. This problem can be encountered when using 3GPP interfaces inside IMS.

## 4. DIAMETER EVOLUTION

Although the protocol has been published in 2003 [RFC3588], a lot of work on updates or extensions are under way. An RFC3588bis document is in preparation, new applications or extensions of the base protocol are in progress. The DIME (Diameter Maintenance and Extensions) working group inside IETF is in charge of the maintenance of the protocol and the Diameter applications specified by IETF. Organizations like 3GPP, 3GPP2 or ETSI/TISPAN also have activities on Diameter, but they are focused on the definition of new diameter applications and usage.

The [RFC3588bis] introduces a lot of precisions that were not present in the initial [RFC3588] and also few evolutions that will not be backward compatible. This document is under discussion within the DIME group for several months. The main explanations added are listed bellow. A lot of them are linked with problems encountered during interoperability.

The usage of the M-bit in the AVP of the Diameter messages (that we have discussed in the previous chapters) is one of them. The confusion between an AVP that is required to be present and an AVP that is required to be understood (which is the definition of this flag) is clearly removed. The restriction concerning the support of accounting for all Diameter application is also removed. The management of the default behavior of the authentication

state machine is given in a more definite way. A lot of incoherencies concerning the accounting application support are solved.

The two following points are also addressed by the [RFC3588bis] document but break backward compatibility. The first one is about the TLS negotiations which will be no longer done within the context of capabilities exchange. TLS is proposed to be established prior to any Diameter traffic via a well known port. The second point concerns the capabilities exchange phase and the way to manage an update of the list of the diameter applications that are supported by a node.

A clarification is needed concerning the realm based routing mechanism defined in the [RFC3588]. A separate internet draft is dedicated to this point. It consists in the definition of rules to determine the administrative domain concerned by a command for the routing using the user level identification.

With the evolution of the protocol itself, new application or extensions are also studied. The creation of a new application based on Diameter for the Quality of Service (QoS) is in progress but not yet standardized. Since the QoS is the control of specific resources, like bandwidth or processing power, service interaction applications could benefit from QoS support by the Diameter protocol, especially when service interaction is bound to a particular bandwidth or level of service (often used for important telephony signals). But the Diameter QoS application will provide AAA for quality of service reservations. This means that a reservation request can be authenticated and authorized and that the resources consumed are accounted for. The quality of service request itself must be made by protocols like the Resource Reservation Protocol (RSVP). Using the mechanism of extension of the protocol, there are four new messages created by this application. The first two ones are used for client initiated authorizations requests to the server. The last two ones are used for server-side initiated QoS parameter provisioning, which means that the server is able to update installed QoS parameters.

## 5. CONCLUSION

AAA has a very large role in the architecture of IMS. As the Diameter protocol is widely adopted by 3GPP, it is more and more used and the number of interfaces based on it increase with the new releases. The main specific mechanisms of the protocol are used inside the IMS to provide AAA handling. The advantages of the protocol like extensibility, flexibility, security, inter-domain cooperation, positioning compared to previous protocols are the major reasons. But the methods used to create this protocol also explain this success: the Diameter protocol was created with different goals. The first one is the resolution of the issues remained open by RADIUS. The construction of the protocol also follows the recommendations for AAA protocols taken from several years of interoperability experiences and regrouped inside different RFCs like [RFC 3127] or [RFC 3539]. Even if it represents an enhancement compared with the previous one, the Diameter protocol is not perfect and some problems appear during interoperability. These problems are going to be solved in the future versions.

The number of applications using Diameter is growing: a lot of interfaces defined for 4G/LTE are based on Diameter and the AAA domain is not the only one where the protocol can be used.

## 6. REFERENCES

### 6.1. IETF REFERENCES

- [RFC 2748] The COPS (Common Open Policy Service) Protocol, January 2000
- [RFC 2904] AAA Authorization Framework, August 2000
- [RFC 3127] Authentication, Authorization and Accounting: Protocol evaluation, June 2001
- [RFC 3539] Authentication, Authorization and Accounting (AAA) Transport profile, June 2003
- [RFC 3588] Diameter Base Protocol, September 2003
- [RFC 4004] Diameter Mobile IPv4 Application, August 2005
- [RFC 4005] Diameter Network Access Server Application, August 2005
- [RFC 4006] Diameter Credit Control Application, August 2005
- [RFC 4072] Diameter Extensible Authentication Protocol (EAP) Application, August 2005
- [RFC 4740] Diameter Session Initiation Protocol (SIP) Application, November 2006

### 6.2. 3GPP REFERENCES

- [TS 23.002] Network Architecture
- [TS 29.328][TS 29.329] Sh, Dh interfaces
- [TS 32.225][TS 32.299] Ro, Rf, Gy interfaces
- [TS 32.296] Re interface
- [TS 29.228][TS 29.229] Cx/Dx interface
- [TS 29.211][TS 29.214] Rx interface
- [TS 29.210][TS 29.212] Gx interface
- [TS 29.207] Gq interface
- [TS 29.109][TS 33.220] Zn, Zh, Dz interfaces
- [TS 29.240] MM10 interface
- [TS 29.234] Dw, Wa, Wd, Wx, Wg, Pr, Wm interfaces  
(WLAN 3GPP interworking system)
- [TS 29.272] S6a, S6d, S13 interfaces
- [TS 23.203] Gxa, Gxb, Gxc interfaces
- [TS 29.273] S6b, STa, SWa, SWd, SWm, SWx, H2 interfaces
- [TS 29.215] S9 interface

## 7. GLOSSARY

3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
API	Application Program Interface
AS	Application Server
ARIB	Association of Radio Industries and Businesses (ARIB)
ATIS	Alliance for Telecommunications Industry Solutions
AVP	Attribute-Value Pair

BGCF	Breakout Gateway Control Function
BSF	Bootstrapping Server Function
CA	Certificate Authority
CAMEL	Customized Application Mobile Enhanced Logic
CCSA	China Communications Standards Association (CCSA)
CDF	Charging Data Feature
CN	Core Network
COPS	(Common Open Policy Service)- RFC 2748
CS	Circuit Switched
CSCF	Call Session Control Function
Cx	Diameter interface for interactions between HSS and CSCF
DCCA	Diameter Credit Control Application
DIAMETER	Successor to RADIUS – RFC 3588 – Need for Mobile IP
DSL	Digital Subscriber Line
ETSI	European Telecommunications Standards Institute
FMC	Fixed/Mobile Convergence
FTTH	Fiber to the Home
GGSN	Gateway GPRS Support Node
GSM	Global System for Mobile Communications
HSS	Home Subscriber Server
HTTP	Hyper Text Transfer Protocol
I-CSCF	Interrogating Call Session Control Function
IPsec	IP Security Protocol
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
ITU	International Telecommunication Union
MGCF	Media Gateway Control Function
MGW	Media Gateway
MMS	Multimedia Messaging Service
MRFC	Media Resource Function Controller
MRFP	Media Resource Function Processor
MSF	MultiService Forum
NAF	Network Application Function

NASREQ	Network Access Server Requirements
NAT	Network Address Translation
NGN	Next Generation Networking
OCF	Online Charging System
OFCS	Offline Charging System
OSA	Open Services Architecture
PRACK	Provision Response Acknowledgement (SIP Message)
P-CSCF	Proxy-Call Session Control Function
PSTN	Public Switched Telephone Network
PDF	Policy Description Function
PDG	Packet Data Gateway
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
QoS	Quality of Service
RADIUS	RFC 2865 - Remote Authentication Dial In User Service
RFC	Request For Comments
SCS	Service Capability Server
S-CSCF	Serving-Call Session Control Function
SCTP	Stream Control Transmission Protocol
SEG	Security Gateway
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLF	Subscriber Location Function
Sh	User profile interface between HSS and AS
TCP	Transmission Transport Protocol
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
TLS	Transport Layer Security
TLV	Type Length Value
TTA	Telecommunications Technology Association (TTA)
TTC	Telecommunication Technology Committee
UE	User Equipment (IMS Terminal)
UMTS	Universal Mobile Telecommunication System
VCC	Voice Call Continuity
VoIP	Voice over IP



WIFI	Wireless Fidelity (IEEE 802.11)
WI-MAX	Worldwide Interoperability for Microwave Access, Inc (IEEE 802.16)
WLAN	Wireless Local Area Network
XCAP	XML Configuration Access Protocol

## Marben Products

For more than 25 years, Marben has been providing key software solutions to telecom equipment manufacturers and services application providers for next generation service-driven networks. We deliver interoperable, robust and efficient solutions to help our customers accelerate their time to market. Our key products include:

- MPLS/GMPLS control plane solution to improve the network capability and to offer new added-value services (fast path provisioning, bandwidth on demand...);
- AAA solution to quickly connect your application to IMS and NGN control plane for dealing with Authentication, QoS, Policy and intelligent charging services;
- Efficient ASN.1 and XML data optimization tools to speed up the transfer of information over low-bandwidth network.

For more information about Marben Products, go to [www.marben-products.com](http://www.marben-products.com).

