1

Architecture Based on Wi-Fi Access

1.1. Functional architecture

EPS (Evolved Packet System) is the name of the 4G mobile network. It consists of an evolved packet core (EPC) and an evolved universal terrestrial radio access network (E-UTRAN).

The E-UTRAN network presents the LTE (Long-Term Evolution) radio interface to the mobile.

Wi-Fi (Wireless Fidelity) interface is subsequently integrated into the EPS network and is a component of a set of technologies grouped under the term Non-3GPP Access.

Its introduction has an impact on the core network (EPC) architecture, which has several variants depending on the following characteristics:

– Wi-Fi access is trusted or untrusted by the operator;

– mobility is managed by the network or the mobile.

1.1.1. *Architecture based on the S2a interface*

The functional architecture based on the S2a interface corresponds to trusted Wi-Fi access and network-based mobility (Figure 1.1).

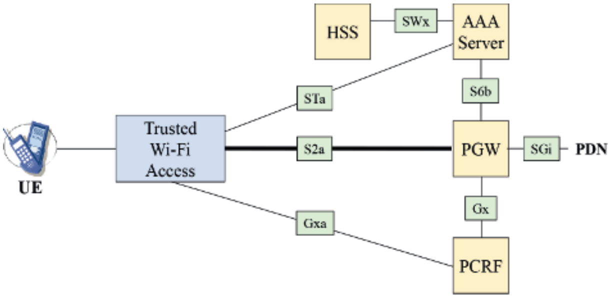

Figure 1.1. *Functional architecture based on the S2a interface*

The mobile stream travels through the Wi-Fi radio interface and the S2a tunnel to access the packet data network (PDN). The PGW (PDN Gateway) entity is an IP (Internet Protocol) router that acts as a gateway for the mobile stream.

The home subscriber server (HSS) and the AAA (Authentication, Authorization and Accounting) server provide the following functions:

– mutual authentication of the mobile and the AAA server via the interfaces SWx and STa. This authentication has the effect of opening Wi-Fi access to the mobile;

– transfer of the mobile profile comprising a list of access point names (APN) and the quality of service (QoS) level of the S2a tunnel and Wi-Fi interface, to the PGW entity, via the interface S6b, and to trusted Wi-Fi access, via the STa interface.

The policy charging and rules function (PCRF) also provides the traffic profile, including the QoS level of the S2a tunnel to the PGW entity, via the Gx interface, and to trusted Wi-Fi access via the Gxa interface.

The mobile profile is stored in the HSS entity for mounting the default bearers, and in this case, the presence of the PCRF is optional.

The presence of the PCRF entity is mandatory for the mounting of dedicated bearers on the initiative of an application function (AF), whose first example of implementation is the VoLTE (Voice over LTE) that provides telephone service.

The characteristics of the dedicated bearer of the IP packet containing the voice are only stored in the SPR (Subscriber Profile Repository) database associated with the PCRF entity.

Trusted WLAN access network (TWAN) includes the following features:

– WLAN AN: this feature includes Wi-Fi access points;

– TWAG (Trusted WLAN Access Gateway): this function terminates tunnel S2a;

– TWAP (Trusted WLAN AAA Proxy): this function terminates the STa interface.

The transparent connection mode provides a single connection to the PGW entity without mobility support between the LTE and Wi-Fi radio accesses. The IPv4 and/or IPv6 address of the mobile is provided by the TWAG function:

– in the case of a statefull configuration, the TWAG function acts as a DHCP (Dynamic Host Configuration Protocol) server;

– in the case of a stateless configuration, the TWAG function broadcasts the prefix of the IPv6 address.

The single-connection mode supports mobility between LTE and Wi-Fi accesses. This mode also supports non-seamless WLAN offload (NSWO), for which traffic is routed directly to the Internet network through TWAG function.

The multiple-connection mode supports NSWO and multiple-access PDN connectivity (MAPCON), for which the various connections to the PDN network pass through the LTE (e.g. telephone service) or Wi-Fi (e.g. Internet service) interfaces according to the policy of the operator. Mobility between LTE and Wi-Fi radio accesses is possible.

The connection on the Wi-Fi interface is established by the WLCP (WLAN Control Plane) protocol. The connection is identified by the MAC address of the mobile associated with a MAC address of the TWAG function.

For the single- or multiple-connection mode, the IPv4 and/or IPv6 address of the mobile is provided by the PGW.

The PGW entity shall allocate the downlink packets to different S2a bearers based on the TFT (Traffic Flow Template) packet filters set up during the establishment of the S2a bearer (Figure 1.2).

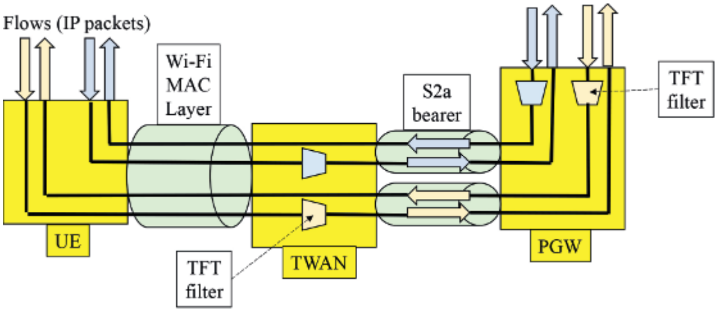

Figure 1.2. *Connection to the PDN network for architecture based on the S2a interface*

TWAN function of the trusted Wi-Fi access shall assign the uplink packets to different S2a bearers based on the TFT packet filters set up during the establishment of the S2a bearer (Figure 1.2).

1.1.2. *Architecture based on the S2b interface*

The functional architecture based on the S2b interface corresponds to untrusted Wi-Fi access and network-based mobility (Figure 1.3).

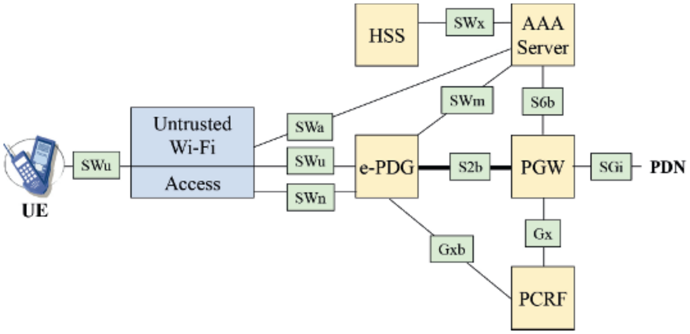

Figure 1.3. *Functional architecture based on the S2b interface*

The mobile stream passes through the SWu and S2b tunnels to access the PDN network via the PGW entity. The SWu tunnel is built between the mobile and the evolved packet data gateway (ePDG). The S2b tunnel is built between the ePDG and PGW entities.

The HSS entity and the AAA server provide the following functions:

– mutual authentication of the mobile and the AAA server, via the SWx and SWa interfaces. This authentication has the effect of opening Wi-Fi access to the mobile;

– mutual authentication related to the establishment of the SWu tunnel, via the SWx and SWm interfaces;

– transfer of the mobile profile comprising a list of access point names (APN) and the quality of service (QoS) level of the S2b tunnel, to the PGW entity via the interface S6b, to the ePDG entity via the SWm interface and to the untrusted Wi-Fi access via the SWa interface.

The PCRF entity provides the QoS level of the S2b tunnel to the PGW via the Gx interface and the ePDG via the Gxb interface.

The PCRF entity provides the QoS level of the SWu tunnel to the ePDG entity via the Gxb interface. In this case, the ePDG entity provides the QoS level to be applied on the Wi-Fi radio interface via the SWn interface.

The mobile must establish a SWu instance for each PDN connection.

When the mobile connects to the PDN network, a default bearer must be established on the S2b interface. This connection is maintained for the duration of the connection.

Dedicated bearers can be built for the same PDN connection, based on the rules provided by the PCRF.

An SWu instance transports the packets of all the S2b bearers for the same connection to the PDN network between the mobile and the ePDG entity.

The ePDG entity shall release the SWu instance when the S2b default bearer of the associated connection to the PDN network is released.

Two IPv4 and/or IPv6 addresses are assigned to the mobile:

– an address for the SWu tunnel built between the mobile and the ePDG entity, provided by the untrusted Wi-Fi access;

– an address for the flow transiting in this tunnel, provided by the PGW entity.

The connection to the PDN network is described in Figure 1.4.

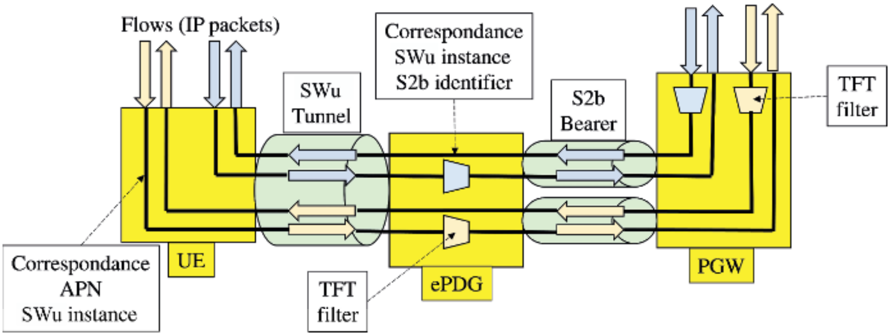

Figure 1.4. *Connection to the PDN network for architecture based on S2b interface*

The PGW entity must allocate the downlink packets to different S2b bearers according to the TFT packet filters set up during the establishment of the S2b bearer.

The ePDG entity must assign the downlink packets to the SWu instance based on the correspondence between the SWu instance and the identifier of the S2b bearer.

The mobile must assign the uplink packets to the SWu instance based on the correspondence between the APN identifier of the PDN connection and the SWu instance.

The ePDG entity must allocate the uplink packets to different S2b bearers according to the TFT packet filters set up during the establishment of the S2b bearer.

1.1.3. *Architecture based on the S2c interface*

The functional architecture based on the S2c interface corresponds to a mobility based on the mobile. The functional architecture is depicted in Figure 1.5 for trusted Wi-Fi access and Figure 1.6 for untrusted Wi-Fi access.

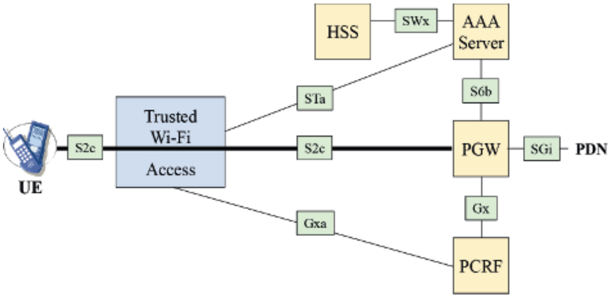

Figure 1.5. *Functional architecture based on S2c interface Trusted Wi-Fi access*

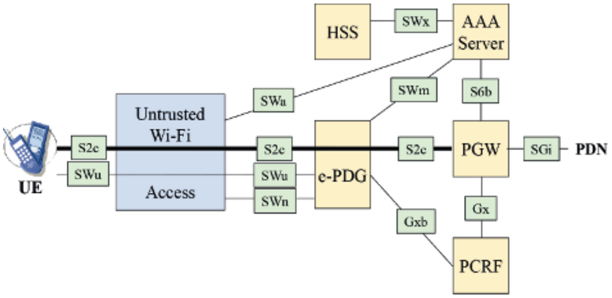

Figure 1.6. *Functional architecture based on S2c interface Untrusted Wi-Fi access*

The mobile stream passes through the S2c tunnel built between the mobile and the PGW entity to access the PDN data network.

In the case of untrusted Wi-Fi access, the S2c tunnel passes through the SWu tunnel built between the mobile and the ePDG entity.

1.2. Tunnel establishment

1.2.1. *Architecture based on the S2a interface*

The S2a interface is the point of reference between the PGW entity and the trusted Wi-Fi access. This interface supports several mechanisms for the establishment of the S2a tunnel.

The construction of S2a tunnel requires the selection of the PGW entity by Wi-Fi access, from information provided by the AAA server during authentication.

This information can be the IP address of the PGW entity, the full qualified domain name (FQDN) or the APN. Trusted Wi-Fi access retrieves the IP address of the PGW entity by performing DNS (Domain Name System) resolution on the FQDN or APN.

1.2.1.1. *PMIPv6 mechanism*

The PMIPv6 (Proxy Mobile IP version 6) mechanism relies on the signaling provided by the mobility extension of the IPv6 header exchanged between Wi-Fi access and the PGW entity (Figure 1.7) and on the GRE (Generic Routing Encapsulation) tunnel of the mobile stream (Figure 1.8).

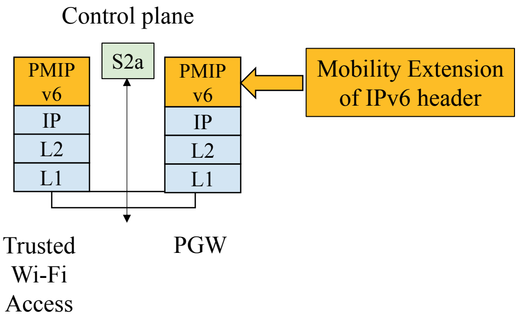

Figure 1.7. *Protocol architecture based on S2a interface Control plane for PMIPv6 mechanism*

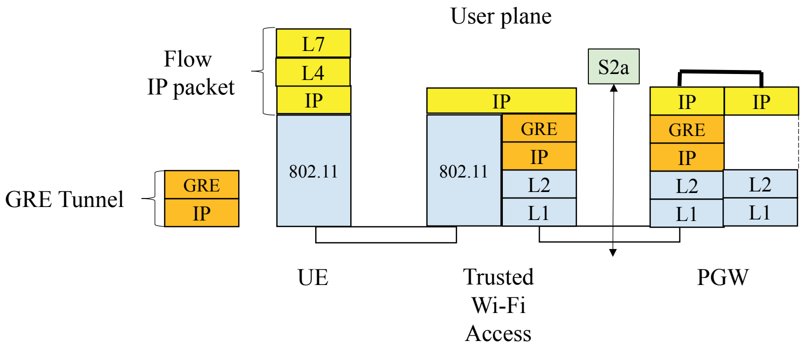

Figure 1.8. *Protocol architecture based on S2a interface User plane for PMIPv6 mechanism*

The MIPv6 mechanism requires functionality in the IPv6 stack of a mobile node. The exchange of signaling messages between the mobile node and the home network agent makes it possible to create and maintain a correspondence between its address in the home network and the foreign network.

Network-based mobility supports the mobility of IPv6 nodes without mobile involvement by extending MIPv6 signaling between the TWAG function and the PGW entity.

This approach to support mobility does not require the mobile node to be involved in the exchange of signaling messages. The PMIPv6 protocol is an extension of the MIPv6 protocol.

A mobile node can operate in an IPv4, IPv6 or IPv4/IPv6 environment. The PMIPv6 protocol independently supports the mobility of the IPv4 address and the transport of IP packets in an IPv4 network.

1.2.1.2. *MIPv4 mechanism*

The MIPv4 FA (Mobile IP version 4 Foreign Agent) mechanism is based on MIPv4 signaling (Figure 1.9) and the IP in the IP tunnel of the mobile stream (Figure 1.10).

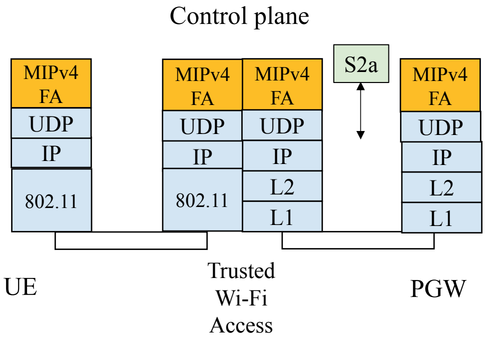

Figure 1.9. *Protocol architecture based on S2a interface Control plane for MIPv4 FA mechanism*

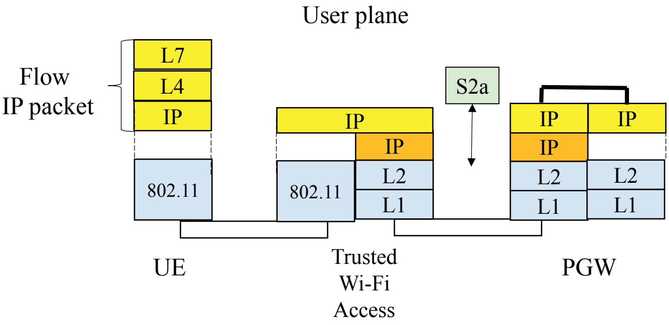

Figure 1.10. *Protocol architecture based on S2a interface User plane for MIPv4 FA mechanism*

MIPv4 signaling is exchanged, on the one hand, between the mobile and trusted Wi-Fi access and, on the other hand, between the trusted Wi-Fi access and the PGW entity.

The MIPv4 protocol allows Wi-Fi access, playing the role of a foreign agent, to assign the mobile an IPv4 address in a foreign network.

The MIPv4 protocol makes it possible to register with the PGW entity, which plays the role of a home agent, the correspondence between the mobile IPv4 address in the home network, provided by the PGW entity, and the IPv4 address in the foreign network.

1.2.1.3. *GTPv2 mechanism*

The GTPv2 (GPRS Tunneling Protocol version 2) mechanism is based on the GTPv2-C (Control) signaling exchanged between the trusted Wi-Fi access and the PGW entity (Figure 1.11) and on the GTP-U (User) tunnel of the mobile flow (Figure 1.12).

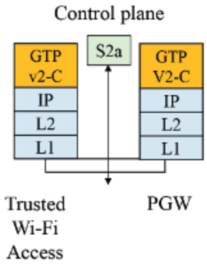

Figure 1.11. *Protocol architecture based on S2a interface Control plane for GTPv2 mechanism*

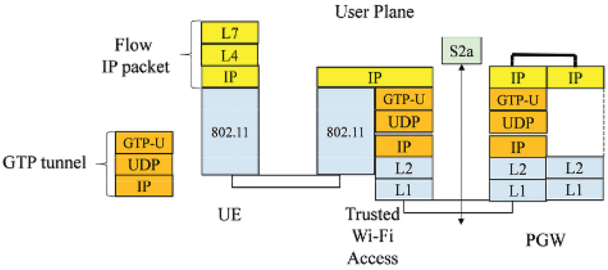

Figure 1.12. *Protocol architecture based on S2a interface User plane for GTPv2 mechanism*

The GTPv2-C protocol allows the activation or deactivation of a session as well as the creation, modification or release of GTP-U bearers.

The PMIPv6 and GTPv2 mechanisms can transport IPv4 or IPv6 streams in IPv4 or IPv6 tunnels. The MIPv4 mechanism allows the transport of only IPv4 streams in IPv4 tunnels.

1.2.2. *Architecture based on the S2b interface*

The S2b interface is the point of reference between the PGW and ePDG entities. This interface supports the PMIPv6 (Figures 1.13 and 1.14) or GTPv2 mechanism for the establishment of the S2b tunnel.

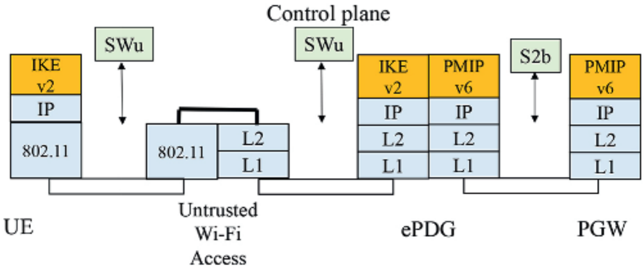

Figure 1.13. *Protocol architecture based on S2b interface Control plane for PMIPv6 mechanism*

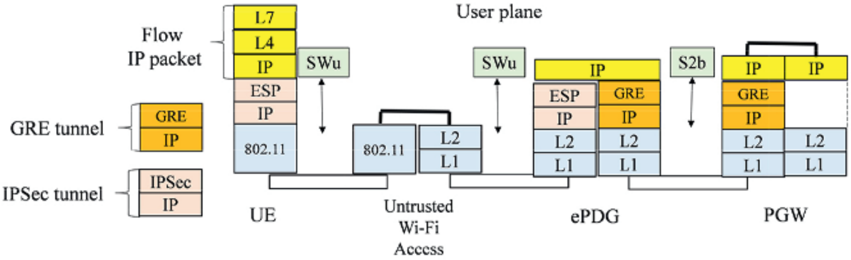

Figure 1.14. *Protocol architecture based on S2b interface User plane for PMIPv6 mechanism*

The SWu interface is the point of reference between the ePDG entity and the mobile. This interface supports the IPSec (IP Security) mechanism, including IKEv2 (Internet Key Exchange version 2) signaling (Figure 1.13) and the ESP (Encapsulating Security Payload) tunnel of the mobile stream (Figure 1.14).

The construction of the SWu tunnel requires the retrieval of the IP address of the ePDG entity by the mobile. This IP address can be configured in the mobile by various means.

The mobile can also perform a DNS resolution on the FQDN of the ePDG entity. The mobile automatically builds the FQDN from the identity of the operator contained in its international mobile subscriber identity (IMSI) or from the tracking area identifier (TAI), where the mobile is located.

The construction of the S2b tunnel requires the selection of the PGW entity by the ePDG entity, from information provided by the AAA server during the authentication for the establishment of the SWu tunnel.

1.2.3. *Architecture based on the S2c interface*

The S2c interface is the point of reference between the PGW entity and the mobile. This interface supports the DSMIPv6 (Dual-Stack Mobile IP version 6) mechanism for the establishment of the S2c tunnel built between the mobile and the PGW entity.

In the case of trusted Wi-Fi access, this interface supports DSMIPv6 signaling (Figure 1.15) and IP in IP tunnel (Figure 1.16) of the mobile stream.

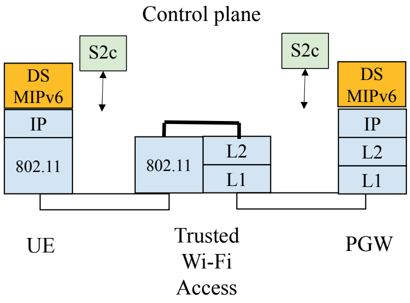

Figure 1.15. *Protocol architecture based on S2c interface Control plane for trusted Wi-Fi access*

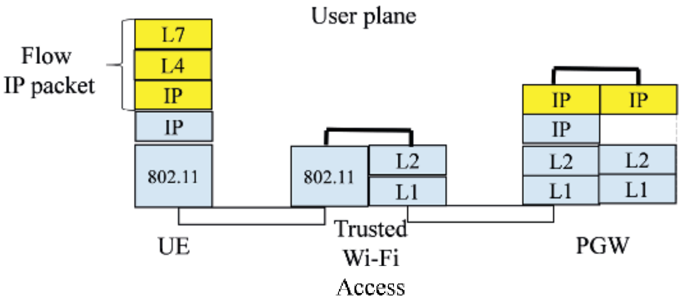

Figure 1.16. *Protocol architecture based on S2c interface User plane for trusted Wi-Fi access*

In the case of untrusted Wi-Fi access, the IPSec tunnel established between the mobile and the ePDG entity protects the S2c interface.

The MIPv6 protocol allows IPv6 mobile nodes to move while maintaining accessibility and ongoing sessions.

The DSMIPv6 protocol prevents the IPv4/IPv6 dual-stack mobile from running both MIPv4 and MIPv6 mobility protocols simultaneously.

The DSMIPv6 protocol also takes into account the case where the mobile moves in a private IPv4 network. The mobile node must be able to communicate with the PGW entity, which acts as a home agent, through a NAT (Network Address Translation) device.

In the case of untrusted Wi-Fi access, the S2c tunnel is established from the IP address of the PGW provided by the AAA server during the authentication for the establishment of the SWu tunnel.

The mobile can also retrieve the IP address of the PGW entity by querying a DHCP (Dynamic Host Configuration Protocol) server or by performing DNS resolution on the FQDN of the PGW.

1.3. DIAMETER protocol

The DIAMETER protocol is used to perform authentication, authorization and accounting functions.

The authentication function makes it possible to control the access of the mobile to the 4G mobile network from a stored secret, on the one hand, in the universal subscriber identity module (USIM) of the universal integrated circuit card (UICC) of the mobile and, on the other hand, in the HSS entity.

The authorization function retrieves the service and traffic profile of the mobile stored in the HSS and SPR databases.

The accounting function allows generation of events from the PGW entity to the charging entities for the prepaid or postpaid service.

1.3.1. *AAA server interfaces*

The DIAMETER protocol is supported on the interfaces between, on the one hand, the AAA server and, on the other hand (Figure 1.17):

– trusted Wi-Fi access via the STa interface;

– untrusted Wi-Fi access via the SWa interface;

– PGW entity via the S6b interface;

– ePDG entity via the SWm interface;

– HSS entity via the SWx interface.

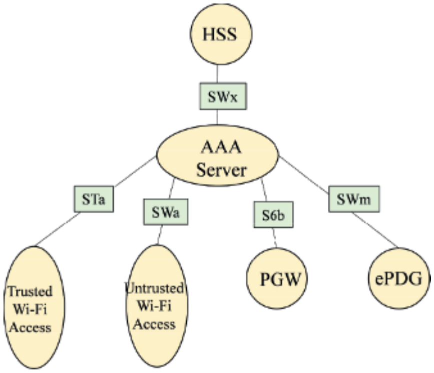

Figure 1.17. *AAA server interfaces using the DIAMETER protocol*

The SWx interface is used by the AAA server to retrieve the authentication data; the subscriber profile and the parameters for the PMIPv6, MIPv4 FA, GTPv2 and DSMIPv6 mechanisms.

The SWx interface is used to register the address of the PGW and the AAA server in the HSS when establishing tunnel S2a, S2b or S2c.

The SWx interface is used by the HSS entity for updating the mobile profile and for detaching it.

Table 1.1 summarizes the DIAMETER messages exchanged on the SWx interface.

Messages	Comments
Multimedia-Authentication-Request (MAR)	AAA server request to retrieve authentication data
Multimedia-Authentication-Answer (MAA)	HSS entity response containing authentication data
Server-Assignment-Request (SAR)	AAA server request to register the PGW entity and retrieve the mobile profile
Server-Assignment-Answer (SAA)	HSS entity response containing mobile profile
Registration-Termination-Request (RTR)	HSS server request for mobile detachment
Registration-Termination-Answer (RTA)	AAA server response to RTR request
Push-Profile-Request (PPR)	HSS entity request for mobile profile update
Push-Profile-Answer (PPA)	AAA server response to PPR request

Table 1.1. *DIAMETER messages on the SWx interface*

The STa and SWa interfaces share the same authentication procedure. During the authentication phase, the AAA server decides whether Wi-Fi access is trusted or untrusted and communicates the decision to the Wi-Fi access point.

The STa and SWa interfaces are used to carry information relating to the PMIPv6, MIPv4 FA (only in the case of the STa interface), GTPv2 and DSMIPv6 mechanisms.

The STa and SWa interfaces are used for detaching the mobile, the procedure being at the initiative of the Wi-Fi access or the AAA server.

The STa and SWa interfaces are used to renew mobile authentication. The procedure is initiated by the AAA server in the event that the subscriber's profile stored in the HSS entity is changed, or at the initiative of the Wi-Fi access that wants to verify that the subscriber's profile is not modified.

Table 1.2 summarizes the DIAMETER messages exchanged on the STa and SWa interfaces.

Messages	Comments
Authenticate and Authorize Request (AAR)	Wi-Fi access request to register and retrieve the mobile profile
Authenticate and Authorize Answer (AAA)	AAA server response containing mobile profile
Re-Auth-Request (RAR)	AAA server request for mobile authentication renewal
Re-Auth-Answer (RAA)	Response from Wi-Fi access to RAR request
Session Termination Request (STR)	Wi-Fi access request for ending the mobile session
Session Termination Answer (STA)	AAA server response to STR request
Abort-Session-Request (ASR)	AAA server request for termination of mobile session
Abort-Session-Answer (ASA)	Response from Wi-Fi access to ASR request
Diameter-EAP-Request (DER)	Wi-Fi access request used for the EAP-AKA authentication procedure
Diameter-EAP-Answer (DEA)	AAA server response used for the EAP-AKA authentication procedure

Table 1.2. *DIAMETER messages on the STa and SWa interfaces*

The S6b interface is used by the PGW entity to communicate to the AAA server its address when the tunnel S2a, S2b or S2c is established.

The S6b interface is used by the PGW entity to retrieve the subscriber's profile and the PMIPv6 and GTPv2 mechanism information.

The S6b interface is used by the PGW entity to retrieve mobile authentication data for the DSMIPv6 mechanism. The authentication data is used to control the establishment of the IPSec mechanism to protect the DSMIPv6 signaling exchanged between the mobile and the PGW entity.

The S6b interface is used for terminating the mobile session, the procedure being initiated by the PGW entity or the AAA server.

Table 1.3 summarizes the DIAMETER messages exchanged on the S6b interface.

Messages	Comments
Authenticate and Authorize Request (AAR)	PGW entity request to register and retrieve the mobile profile
Authenticate and Authorize Answer (AAA)	AAA server response containing mobile profile
Re-Auth-Request (RAR)	AAA server request for mobile authentication renewal
Re-Auth-Answer (RAA)	PGW response to RAR request
Session Termination Request (STR)	PGW request for termination of mobile session
Session Termination Answer (STA)	AAA server response to STR request
Abort-Session-Request (ASR)	AAA server request for termination of mobile session
Abort-Session-Answer (ASA)	PGW response to ASR request
Diameter-EAP-Request (DER)	Request of the PGW entity used for the EAP-AKA authentication procedure for the DSMIPv6 mechanism
Diameter-EAP-Answer (DEA)	AAA server response used for the EAP-AKA authentication procedure

Table 1.3. *DIAMETER messages on the S6b interface*

The SWm interface is used for the mutual authentication procedure of the mobile and the AAA server, which is implemented during the establishment of the SWu tunnel.

The SWm interface is used by the ePDG entity to retrieve the subscriber's profile and the PMIPv6 and GTPv2 mechanism information.

The SWm interface can also be used to transmit to the ePDG entity, the IP address or the FQDN of the PGW entity.

The SWm interface is used for terminating the mobile session, the procedure being initiated by the ePDG entity or the AAA server.

Table 1.4 summarizes the DIAMETER messages exchanged on the SWm interface.

Messages	Comments
Authenticate and Authorize Request (AAR)	Request from the ePDG entity to register itself and retrieve the mobile profile
Authenticate and Authorize Answer (AAA)	AAA server response containing mobile profile
Re-Auth-Request (RAR)	AAA server request for mobile authentication renewal
Re-Auth-Answer (RAA)	Response of the ePDG entity to the RAR request
Session Termination Request (STR)	Request from ePDG entity for termination of mobile session
Session Termination Answer (STA)	AAA server response to STR request
Abort-Session-Request (ASR)	AAA server request for termination of mobile session
Abort-Session-Answer (ASA)	Response of the ePDG entity to the ASR request
Diameter-EAP-Request (DER)	Request of the ePDG entity used for the EAP-AKA authentication procedure for the DSMIPv6 mechanism
Diameter-EAP-Answer (DEA)	AAA server response used for the EAP-AKA authentication procedure

Table 1.4. *DIAMETER messages on the SWm interface*

1.3.2. *PCRF interfaces*

The DIAMETER protocol is also supported on the interfaces between, on the one hand, the PCRF entity and, on the other hand (Figure 1.18):

– PGW entity via the Gx interface;

– trusted Wi-Fi access via the Gxa interface;

– ePDG entity via the Gxb interface.

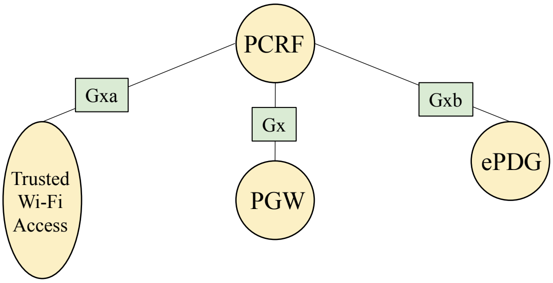

Figure 1.18. *PCRF interfaces using the DIAMETER protocol*

The Gx, Gxa and Gxb interfaces make it possible to request the PCRF entity to:

– retrieve the rules to apply to the default bearer created by the EPS network;

– inform the PCRF entity of the termination of the session on the EPS network.

The Gx, Gxa and Gxb interfaces allow the PCRF entity to provide the rules to be applied for the dedicated bearer.

Table 1.5 summarizes the DIAMETER messages exchanged on the Gx, Gxa and Gxb interfaces.

Messages	Comments
Credit-Control-Request (CCR)	Request from PGW, ePDG or trusted Wi-Fi entities to retrieve the mobile profile
Credit-Control-Answer (CCA)	PCRF response containing the mobile profile
Re-Auth-Request (RAR)	Request from the PCRF entity containing the mobile profile
Re-Auth-Answer (RAA)	Response of PGW, ePDG or trusted Wi-Fi access to the RAR request

Table 1.5. *DIAMETER messages on the Gx, Gxa and Gxb interfaces*