Radiator

3GPP AAA Server

Radiator Software Oy

For Radiator SIM Pack 2.9

27.8.2024

Abstract

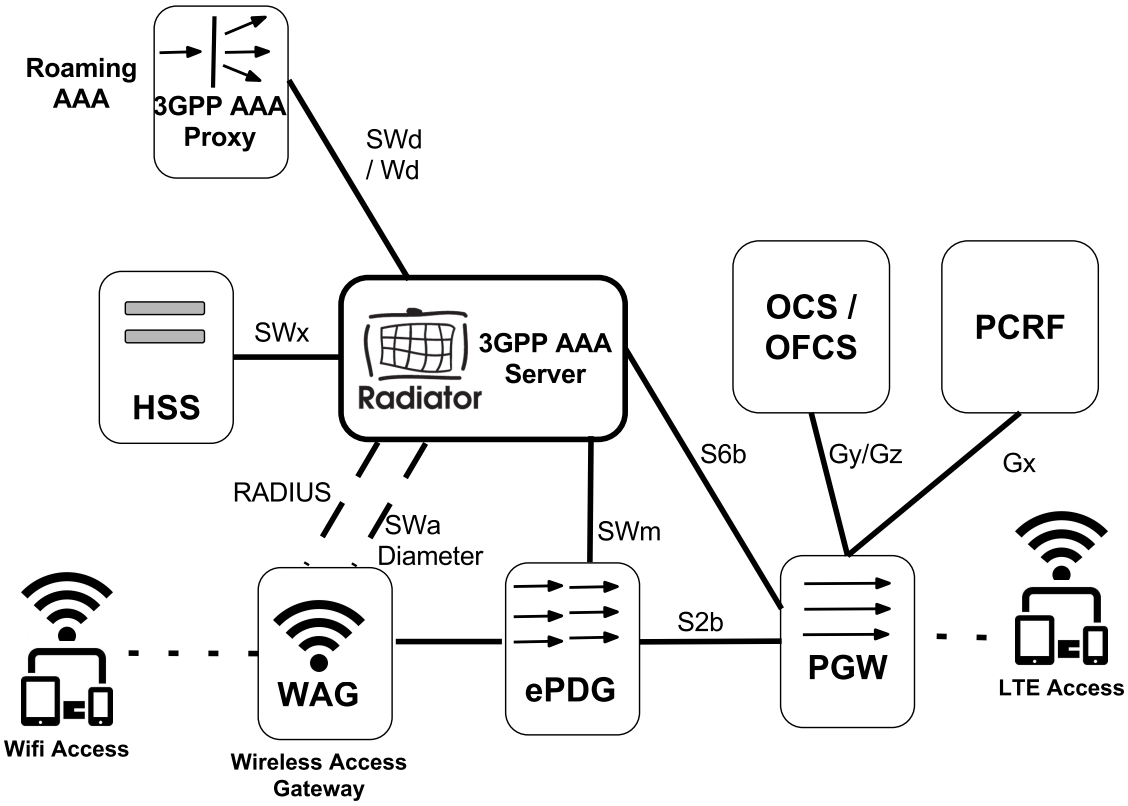
This document describes the architecture and technical functionality of a 3GPP AAA Server. Also 3GPP AAA Server use cases, VoWiFi and Wi-Fi offloading, are introduced. The last section has a short introduction of Radiator SIM Pack which contains the 3GPP AAA Server.

Table of Contents

1. Introduction of 3GPP AAA Server

This section describes the architecture of the 3GPP AAA Server and its basic functionality.

Figure 1. Untrusted non-3GPP access architecture



The 3GPP AAA Server provides the AAA (Authentication, Authorisation, Accounting) functionality to allow non-3GPP access, such as Wi-Fi, to the operator's EPC (Evolved Packet Core). Thus, it makes possible to use non-3GPP connections, both trusted and untrusted, for services that require user authentication. These services include VoWiFi (Voice over Wi-Fi) and Wi-Fi offloading, among others. In a roaming situation, the 3GPP AAA Server also acts as a proxy server. Figure 1 shows the basic architecture of a non-3GPP access system.

The 3GPP AAA Server's authentication function provides a reliable way to identify the user. Typically in other systems, the authentication is done by entering a valid user name and password. The 3GPP AAA Server uses SIM-based authentication which is easier, more secure, and more flexible as it does not require a separate user name and password. The 3GPP AAA Server uses the operator's HSS (Home Subscriber Server) and does not require a separate user information database.

The authorisation function determines if the authenticated user has access rights for using services, which require 3GPP access, and enforces the subscriber profile. The profile contains usage policies, charging information, and other connection details, such as bandwidth restrictions or whether the subscriber is allowed to use a certain Wi-Fi APN (access point name). The 3GPP AAA Server retrieves the authorisation data from the HSS.

The accounting function measures the used resources. However, the 3GPP AAA Server is not used for accounting. The PDN GW (Packet Data Network Gateway) transfers the accounting data directly to either OFCS (offline charging system), OCS (online charging system), or PCRF (policy and charging rules function) as it is shown in Figure 1.

2. 3GPP AAA Server functionality

This section explains the 3GPP AAA Server's role in the following actions:

- Connecting via untrusted non-3GPP access network
- Disconnecting from untrusted non-3GPP access network
- Updating the subscriber profile

2.1. Connecting via non-3GPP access network

Figure 2. Authentication and authorisation in untrusted non-3GPP access network

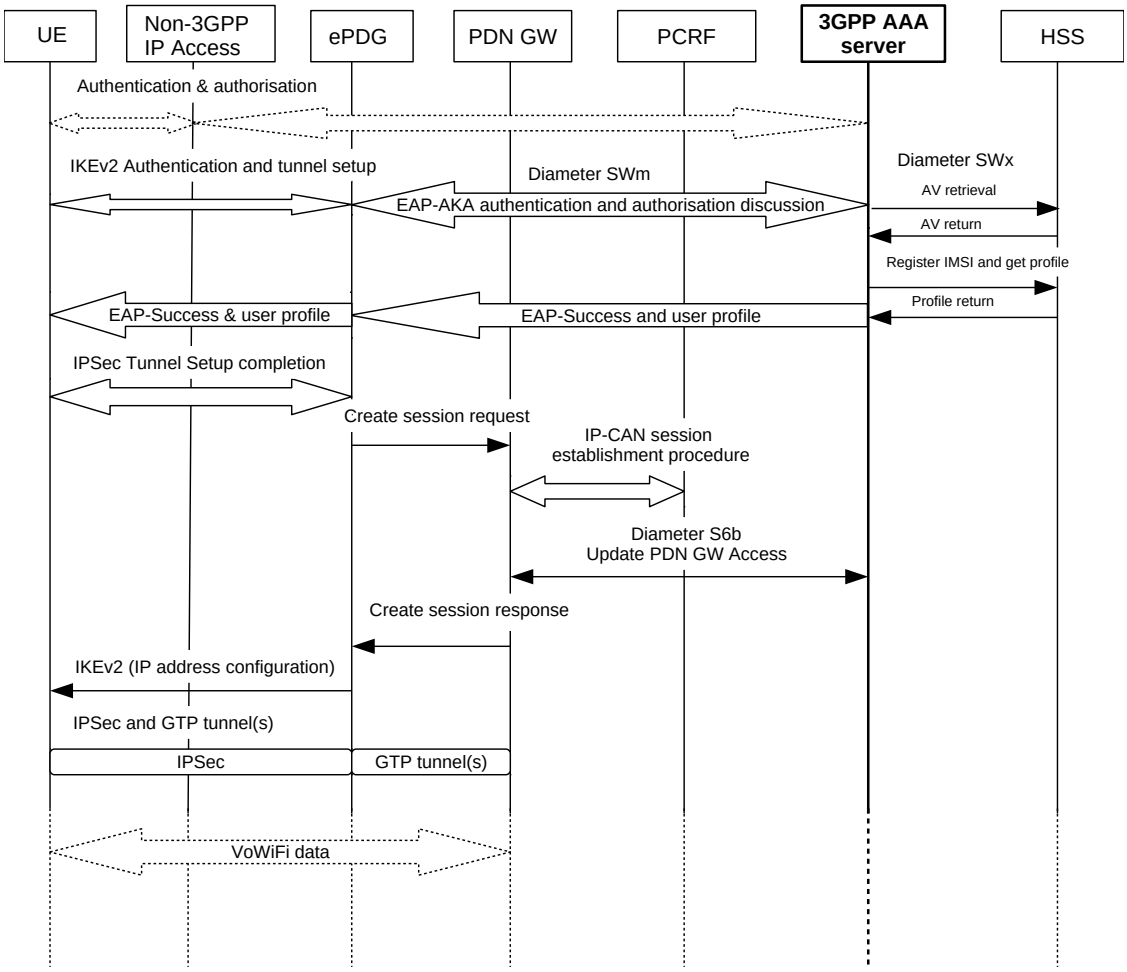


Figure 2 describes the procedure how a UE (user equipment) connects to a service that requires usage of EPC services, such as IMS (IP Multimedia Subsystem) in VoWiFi, via non-3GPP access:

1. The UE sets up an IKEv2 connection to the ePDG (evolved Packet Data Gateway).
2. The UE sends an EAP (Extensible Authentication Protocol) message to the ePDG.
3. The ePDG extracts the EAP message out of an IKEv2 message and sends it to the 3GPP AAA Server via Diameter protocol.
4. The 3GPP AAA Server requests an AV (authentication vector) from the HSS.
5. The 3GPP AAA Server sends an AUTH parameter within the EAP message to the UE.

6. The UE checks the authentication parameters and responds to the authentication request.
7. The ePDG forwards the response from the UE to the 3GPP AAA Server.
8. The 3GPP AAA Server checks if the authentication response is correct.
9. The 3GPP AAA Server retrieves the subscriber profile from the HSS and checks if the user is authorised to use non-3GPP access.
10. The 3GPP AAA Server sends the final authentication and authorisation answer to the ePDG if the check is successful.
11. The ePDG forwards the success message to the UE.

2.2. Disconnecting from non-3GPP access network

Figure 3. UE-initiated session termination from untrusted non-3GPP access network

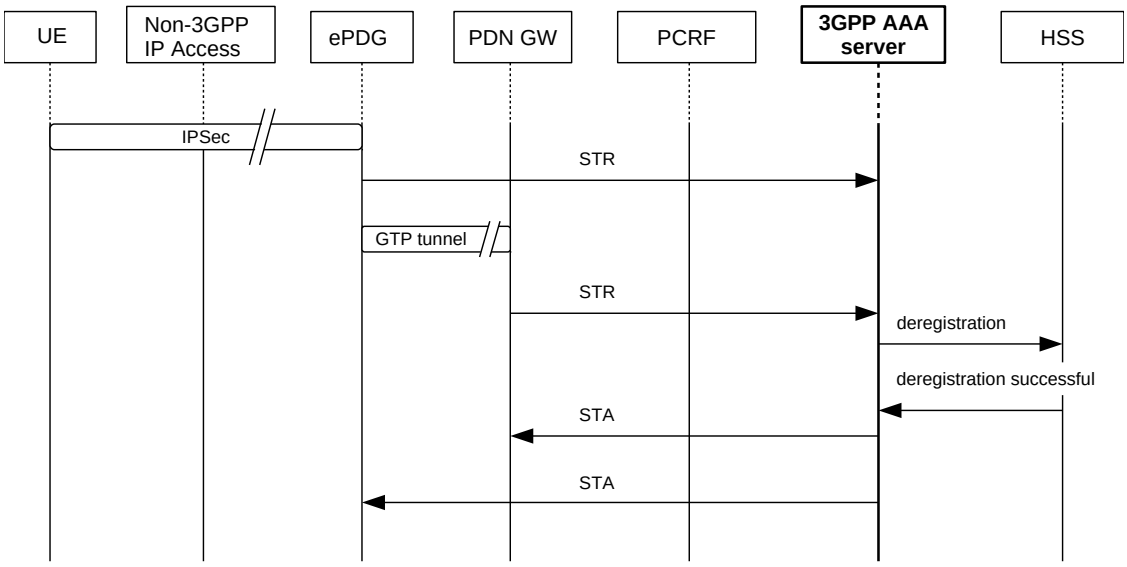


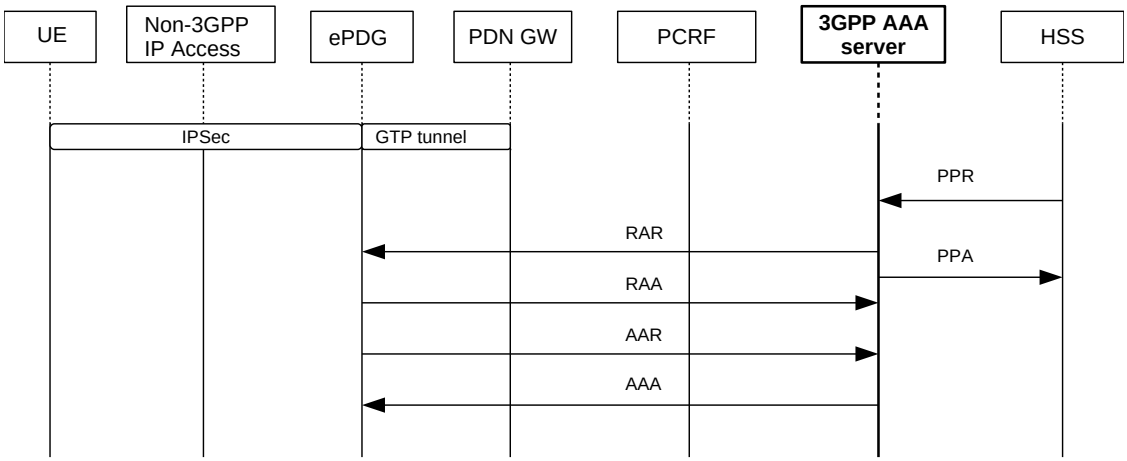
Figure 3 describes the disconnecting procedure when the IPSec tunnel is disconnected, for example, when the UE moves out of Wi-Fi coverage:

1. An STR (Session-Termination-Request) is initiated by the ePDG to the 3GPP AAA Server.
2. The 3GPP AAA Server checks if there is an ongoing session associated to the parameters received via the STR.
3. The PDN GW sends an STR when the GTP tunnel is disconnected.
4. The 3GPP AAA Server checks the session status. If an active session is found, the 3GPP AAA Server removes the associated non-3GPP access information in the HSS.
5. The STAs (Session-Termination-Answers) are sent to both the PDN GW and ePDG.

It is also possible for the HSS to terminate the session via the 3GPP AAA Server. This feature is needed, for example, when the IMSI (international mobile subscriber identity) has been terminated. In this case, the 3GPP AAA Server sends an ASR (Abort-Session-Request) to the ePDG.

2.3. Updating subscriber profile

Figure 4. Subscriber profile updating process



In some cases, the subscriber profile has to be updated for various reasons, such as, when the IMSI is locked or a Wi-Fi APN is not permitted any more. The subscriber profile update process is described in Figure 4. The HSS can update the subscriber profile and its parameters to the ePDG via the 3GPP AAA Server:

1. The HSS sends a PPR (Push-Profile-Request) with the updated subscriber profile to the 3GPP AAA Server.
2. The 3GPP AAA Server initiates a re-authorisation procedure and sends a RAR (Re-Auth-Request) to the ePDG.
3. The 3GPP AAA Server sends a PPA (Push-Profile-Answer) to the HSS.
4. The ePDG answers the RAR with RAA (Re-Auth-Answer).
5. The ePDG requests the re-authentication with an AAR (AA-Request) to be able to apply the new subscriber profile.
6. The 3GPP AAA Server sends an AAA (AA-Answer) to the ePDG after the re-authentication is done.

The following steps, if there are any, depend on the AAA sent to the ePDG. For example, the connection may be terminated.

3. 3GPP AAA Server use cases

This section introduces two important use cases of the 3GPP AAA Server: VoWiFi and Wi-Fi offloading. More 3GPP AAA Server use cases are found in Radiator Cookbook blog [https://blog.radiatorsoftware.com/].

3.1. VoWiFi

Many mobile users prefer Wi-Fi connection to the cellular network. This happens especially when travelling abroad as it reduces the roaming costs. Also the cellular coverage may be poor in indoor areas. VoWiFi offers a solution to use voice calls over Wi-Fi. For operators, VoWiFi provides significant business potential and thus several operators are implementing it. Using Wi-Fi provides a low-cost method to improve voice service coverage in indoor areas.

Providing a native VoWiFi client requires reliable user authentication. Using the 3GPP AAA Server makes it possible to use SIM-based authentication which does not require the user to remember yet another user name and password to get a secure voice call connection. When VoWiFi is provided via a native client with SIM-based authentication, it makes VoWiFi calling very easy, not different than using the ordinary voice calls. SIM-based authentication uses the user credentials provided by the SIM and no separate user profiles are needed.

3.2. Wi-Fi offloading

With Wi-Fi offloading, the operators can transfer traffic from EPC to Wi-Fi networks. It makes possible to build more capacity in an affordable and flexible way. Like VoWiFi, Wi-Fi offloading improves the coverage in indoor areas and thus enhances the user experience. SIM-based authentication provided by the 3GPP AAA Server provides the best way for automatic and seamless user authentication and authorisation.

4. 3GPP AAA Server in Radiator SIM Pack

The 3GPP AAA Server is part of Radiator SIM Pack. Radiator SIM Pack is a component for data and voice roaming between cellular and Wi-Fi networks. It has been developed since 2003 and is currently used by carriers and service providers all around the world. In addition to the 3GPP AAA Server, Radiator SIM Pack includes also the following features:

- All SIM-based authentication standards: EAP-SIM, EAP-AKA, and EAP-AKA’
- M3UA/SIGTRAN for EAP-AKA and EAP-SIM
- 3GPP Diameter interfaces: S6b, SWm, SWa, Wx, and SWx
- AKA vector conversion to SIM triplets
- MAP/SS7 gateways for AuC/HLR connection over MAP, SIGTRAN, and other protocols