EAP-SIM Authentication using Interlink Networks RAD-Series RADIUS Server

Introduction

The demand for wireless LAN (WLAN) access to the public IP network is growing rapidly. It is only natural that digital cellular service providers want to extend their offerings to include data services. By leveraging their existing network, customer service, and billing infrastructure, they can jump start their WLAN business while realizing significant cost savings and operational synergy. Global System for Mobile Communications (GSM) is a standard for digital cellular service throughout Europe, Japan, and other parts of the world. Signaling System 7 (SS7) is the network control protocol used by switches in of GSM and other telecommunications networking systems.

Security, especially controlling access to the network through the use of AAA (Authentication, Authorization, and Accounting) services is essential for both voice and data. This application note presents how Interlink Networks' RAD-Series RADIUS Server can be deployed as a gateway between an IP network and an SS7 network resulting in a shared authentication service for both networks.

Authentication in a GSM Network

Every mobile subscriber is assigned a unique International Mobile Subscriber Identity (IMSI) number, which identifies both the subscriber and their subscription within the GSM network. The IMSI is made up of a 3 digit Mobile Country Code (MCC), a 2 digit Mobile Network Code (MNC), and a 10 digit Mobile Subscriber Identity Number (MSIN). The IMSI resides in a Subscriber Identity Module (SIM), which can be plugged into any Mobile Station Equipment (MSE). The IMSI itself is not dial-able so each subscriber is also assigned dial-able Mobile Subscriber ISDN (MSISDN) numbers. The mapping between IMSI and MSISDN along with a secret shared key, K_i, and other subscriber information is maintained in a database called the Home Location Register (HLR).

As a mobile subscriber roams to other networks, he must be authenticated back to his home network. Figure 1 gives a simple illustration of how GSM SIM authentication takes place.

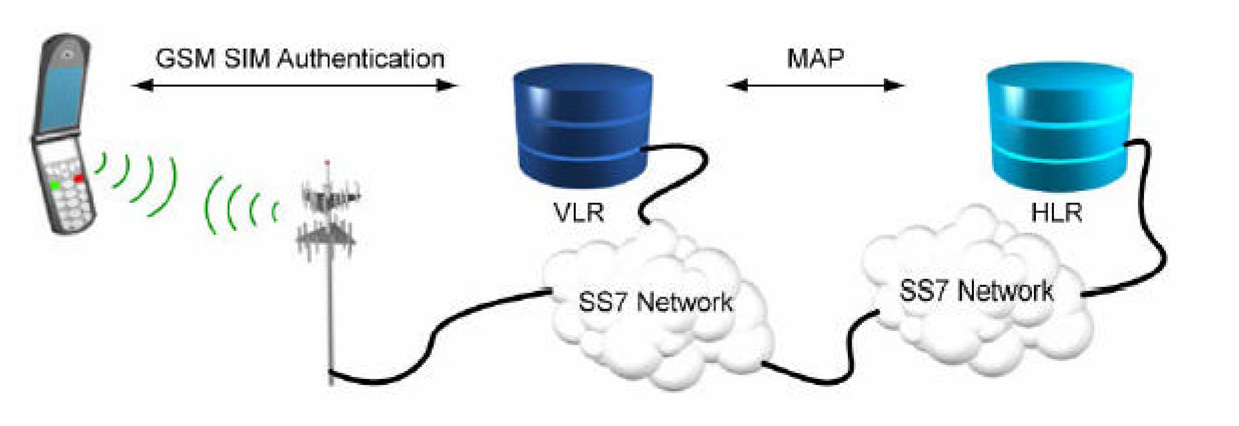


Figure 1. GSM SIM authentication in a GSM network

The mobile user is registered on the foreign network's Visitor Location Register (VLR). From the subscriber's IMSI, the VLR is able to establish communications with the subscriber's HLR through the SS7 network using the Mobile Application Part (MAP) protocol. The VLR sends a MAP SendAuthInfo request with the subscriber's IMSI to the subscriber's HLR. The HLR responds with a MAP SendAuthInfo response with a triplet comprised of

1. A random number challenge
2. A secret response generated using the IMSI, random number, and K_i
3. A session key, K_c

The VLR then challenges the SIM using the random number. If the SIM responds with a secret response matching the one provided by the HLR, then the subscriber is authenticated. Otherwise, the call is rejected.

802.1X Authentication for WLANs

802.1X is the IEEE standard for Port Based Network Access Control. 802.1X insures that only authenticated users are granted access through the controlled port on the access device, also known as the authenticator. The authentication software on the user's station is referred to as the supplicant. Until the user is authenticated, the supplicant can only communicate with the authentication server, using the Extensible Authentication Protocol (EAP). EAP serves as a framework for a variety of authentication methods. The best EAP methods provide mutual authentication where both the supplicant is authenticated to the authentication server and the authentication server is authenticated to the supplicant.

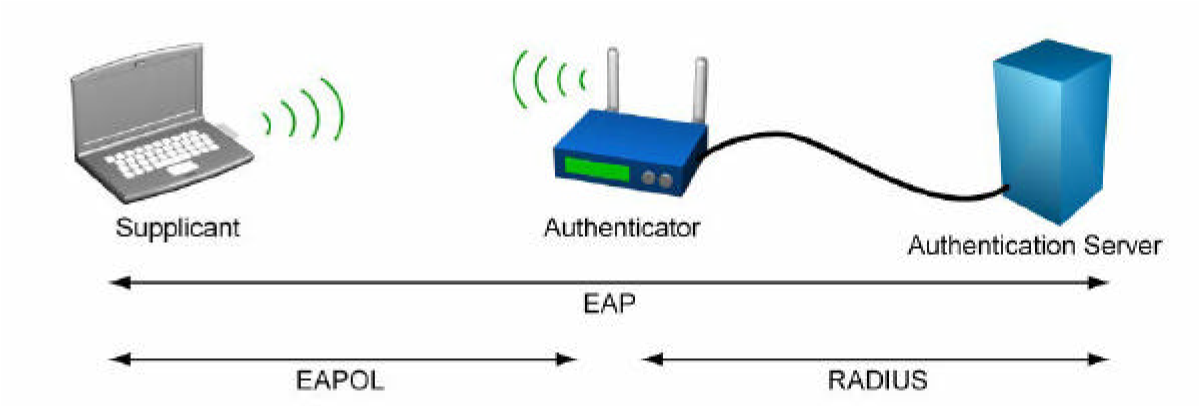


Figure 2. 802.1X authentication using EAP

RAD-Series Architecture for EAP-SIM Authentication

In EAP-SIM, the RAD-Series Server acts as a gateway between the IP and SS7 networks. To the IP network it appears as an authentication server and uses its standard EAP-SIM module to authenticate the user's EAP-SIM supplicant. To the SS7 network it appears as a VLR and communicates by MAP with the HLR using an SS7 plug-in module developed with the EAP-SIM Developer's Kit

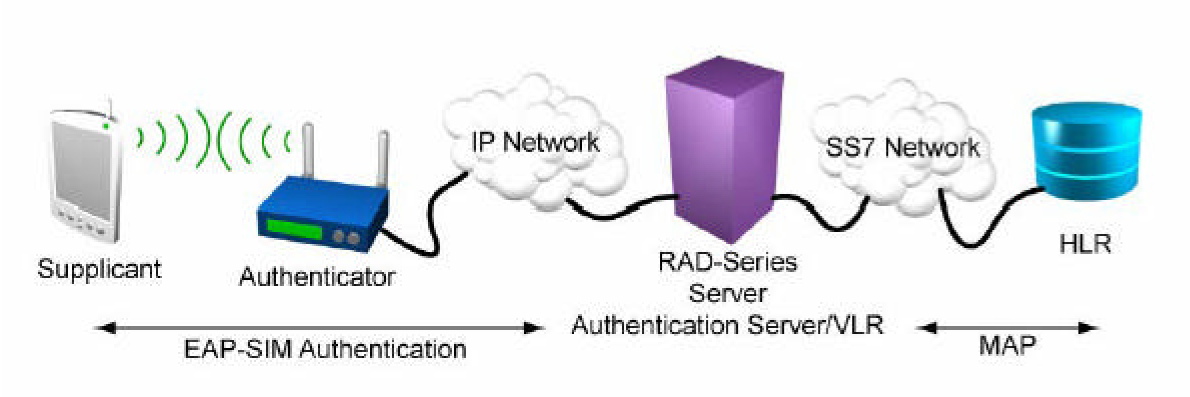
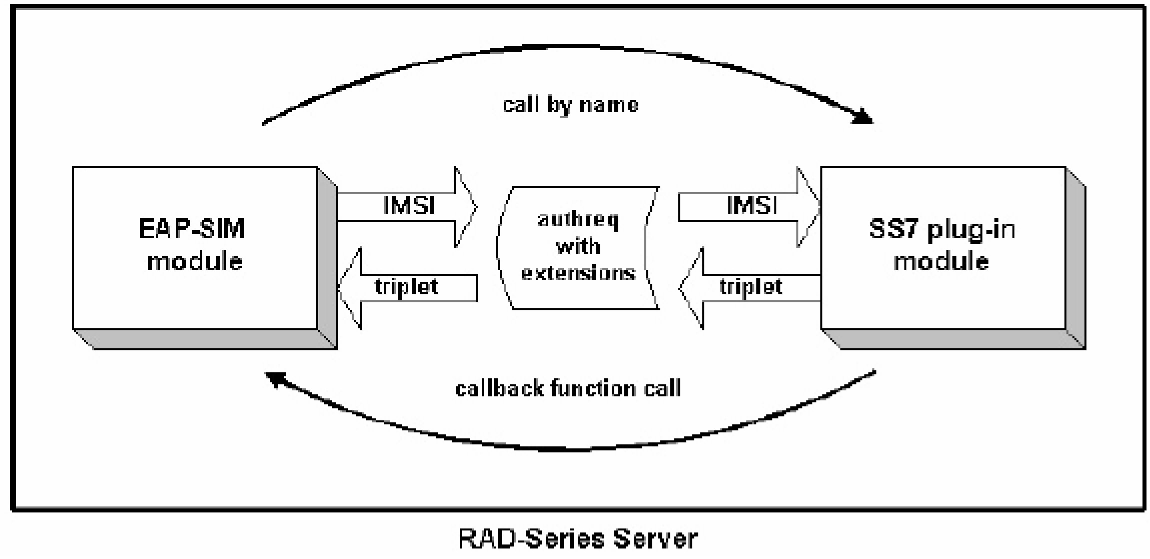


Figure 3. RAD-Series Server acting as authentication gateway between IP and SS7 networks

The SS7 plug-in module has a direct interface to the EAP-SIM module. No modification of the finite state machine table is required. Data is passed between the two modules through a shared extension to the basic authentication processing data structure called an authreq. The SS7 plug-in module is registered in the RAD-Series Server enabling the EAP-SIM module to pass control through an internal call by name function. The EAP-SIM module passes a pointer to its callback function through the authreq extension to the SS7 plug-in module.



Fi

gure 4. EAP-SIM and SS7 plug-in module data and control flow

The process for a successful EAP-SIM authentication will flow as follows:

1. The supplicant associates with the authenticator (access point).
2. The authenticator sends an EAP ID-Request to the supplicant.
3. The supplicant responds with an EAP ID-Response, which is passed through the authenticator to the authentication server (RAD-Series Server).
4. The EAP-SIM plug-in processes the EAP ID-Response to get the subscriber's IMSI.
5. The EAP-SIM module stores the IMSI and callback function pointer in the authreq extension and calls the SS7 plug-in module's action function.
6. The SS7 module sends the MAP SendAuthInfo request with the IMSI to the HLR.
7. The HLR returns to the SS7 plug-in module a MAP SendAuthInfo response including a triplet.
8. The SS7 plug-in maps the response to the appropriate authreq data structure and stores the triplet in the extension.
9. The SS7 plug-in calls the EAP-SIM callback function.
10. The EAP-SIM module uses the triplet to complete a series of EAP-SIM challenges with the supplicant resulting in an EAP-Success.

Interlink Networks EAP-SIM Developer's Kit

The Interlink Networks EAP-SIM Developer's Lot has two components.

1. Interlink Networks' Authentication API

> Interlink Networks' Authentication API contains both the C programming language build environment and the server interface definition needed to develop custom feature modules and plug them into the RAD-Series RADIUS Server. The interface includes both header definitions for data structures and function prototypes for the packet and attribute handling functions that are the building blocks of every plug-in module. The finished product is a shared object that is

dynamically loaded by the RAD-Series Server. At the heart of the RAD-Series architecture is a finite state machine (FSM) making it possible to plug in new functions at any point in the process of handling a RADIUS request.

2. Interlink Networks EAP-SIM and extensions

The EAP-SIM Developer's Kit contains additional header files extending the authentication data structures and defining conditions specific to EAP-SIM processing.

Implementing an SS7 Plug-in

The steps to implement an SS7 plug-in are straightforward.

1. Define the plug-in module

   A macro from the Authentication API is used to define the SS7 plug-in including its name, init function, action function, and receive function.

2. Define a MAP request/response mapping table

   Since multiple simultaneous authentications are possible, the SS7 module must define a table for matching MAP responses to MAP requests and mapping back to the associated authreq data structure.

3. Write the SS7 init function

   The RAD-Series Server calls registered init functions at server startup and in response to a SIGHUP signal. The SS7 plug-in should check for a socket connection to the SS7 network and establish one if none exists.

4. Write the SS7 action function

   The SS7 action function is the function called by the EAP-SIM module once it has the user IMSI and needs a triplet from the HLR in order to proceed with the EAP-SIM authentication. It will also be called if the authentication is to be canceled before a response has been received from the HLR. If the call is an authorization information request then the action function will

   a) generate a MAP SendAuthInfo request using the IMSI from the authreq extension.

   b) enter the request in its request table along with a pointer to the authreq data structure.

   c) transmit the request on the SS7 network socket.

   d) return AAA_EV_WAIT, which puts the finite state machine for the current request into a wait state.

   If the call is a cancellation request then the action function will

   a) flag the MAP request as cancelled in its table

   b) return AAA_EV_NAK, which informs the finite state machine that the authentication has failed.

5. Write the SS7 receive function The SS7 receive function is the function called by the RAD-Series Server when a packet is received on the socket registered for the SS7 plug-in module. The receive function will

    a) match the MAP SendAuthInfo response to a request in its table.

        i. If a match is found then the pointer to the authreq data structure is retrieved.

        ii. If a match is found but flagged as cancelled then the table entry is cleared and AAA_EV_NAK is returned.

        iii. If no match is found then AAA_EV_NAK is returned.

    b) store results from the MAP SendAuthInfo response in the authreq extension.

        i. If the transaction is successful then the triplet is stored.

        ii. If the transaction is unsuccessful then the error codes are stored.

    c) get the EAP-SIM callback function pointer from the authreq and call it.

5. Compile and link the SS7 plug-in.

    The Authentication API configure scripts to determine the system environment are run to generate make files which in turn are run resulting in a shared object.

6. Install SS7 plug-in the RAD-Series Server plug-in directory

    The shared object is copied to the plug-in directory from which it will be loaded when the RAD-Series Server is reloaded.

There is no need for the SS7 plug-in module to allocate or return data structures other than its table for matching MAP responses to requests.

Conclusion

Using Interlink Networks' RAD-Series RADIUS Server as a gateway between the IP network and the SS7 network, a GSM operator can efficiently extend his subscriber authentication infrastructure to manage access to a WLAN service offering. RAD-Series' standard EAP-SIM support makes it possible for GSM subscribers to use a single SIM for both voice and data access. The RAD-Series EAP-SIM Developer's Kit empowers the GSM operator to create a compatible and reliable interface to his SS7 network. The need for a redundant subscriber database and the associated management costs are eliminated while guaranteeing a uniformly secure network for both voice and data services.

INTERLINK NETWORKS

Interlink Networks delivers the most powerful, robust, and scalable RADIUS server solutions on the market. Since 1991, our RAD-Series Servers have provided access management solutions to some of the largest Carrier and Service Providers around the world.

Interlink Networks, LLC.
2500 Packard Rd, Suite 202
Ann Arbor, MI 48104

Main - (734) 821-1200
Sales - (734) 821-1228
Fax - (734) 821-1235