Radiator
EAP-SIM and EAP-AKA Support

White paper discussing EAP-SIM and EAP-AKA authentication support for Radiator.
For EAP-SIM Module version 1.32

1.0 Introduction

This document describes the emerging EAP-SIM and EAP-AKA authentication standard for Wireless LANs, and outlines the support for EAP-SIM and EAP-AKA authentication available with Radiator, the full source Radius server from Open System Consultants (www.open.com.au/radiator).

Radius is the de-facto standard protocol for authenticating users and for recording accounting information for wireless and wired LANs. See RFCs 2138, 2139, 2865 and 2866 for more details on the Radius protocol.

EAP is the Extensible Authentication Protocol, which can be used to create new types of authentication protocols for Radius. See RFCs 2284 and 2869 for more details on EAP authentication for Radius. These new types of authentication are commonly used in Wireless LAN systems.

EAP-SIM RFC 4186 is a newly emerged EAP authentication protocol, designed for use with existing GSM mobile telephone authentication systems and SIMs (Subscriber Identity Modules) for mobile phones. The EAP-SIM standard allows Wireless LAN users to authenticate access to a Wireless LAN network using a mobile phone SIM card. The standard for EAP-SIM authentication is still in draft form with the IETF (Internet Engineering Task Force).

EAP-AKA RFC 4187 is a newly emerged EAP authentication protocol, designed for use with 3GPP authentication system and USIM (Subscriber Identity Modules) cards for mobile phones. EAP-AKA has similar properties and protocols to EAP-SIM. The EAP-AKA standard allows Wireless LAN users to authenticate access to a Wireless LAN network using a 3G mobile phone USIM card.

Even more recently, EAP-AKA' (AKA prime) RFC 5448 has been introduced. It has similar properties to EAP-AKA

Radiator is a highly configurable and extensible Radius server that allows you to easily customize and control how you authenticate users and record accounting information. Radiator supports a wide range of EAP authentication methods, including EAP-MD5, EAP-TLS, EAP-TTLS and EAP-PEAP as part of its standard package. Support for EAP-SIM authentication is available as an add-on package for Radiator.

Using Radiator and its optional EAP-SIM and EAP-AKA support, operators and carriers are able to construct complete EAP-SIM wireless authentication and billing systems, that interoperate with and utilize the existing worldwide GSM mobile phone authentication and billing systems, enabling a simple and seamless use and billing experience for roaming wireless LAN users.

The Radiator EAP-SIM module comes with support for the Performance Technologies (http://www.pt.com) SGSA Map Gateway out of the box. It also includes source code for customizing and interfacing with other third-party MAP gateways.

Support for Cisco ITP MAP Gateway is available on request to qualified Cisco ITP customers.

2.0 What is EAP-SIM?

2.1 Overview

EAP-SIM is a newly emerging standard for authenticating Wireless LAN access with mobile phone SIM cards and the worldwide GSM mobile phone authentication network.

2.2 Standards

The standard for EAP-SIM authentication is contained in RFC 4186 from IETF (www.ietf.org).

The Radiator EAP-SIM module is compatible with RFC 4186, including optional Result Indications as per section 6.2 of RFC 4186.

The Radiator EAP-AKA module is compatible with RFC 4187 and RFC 5448.

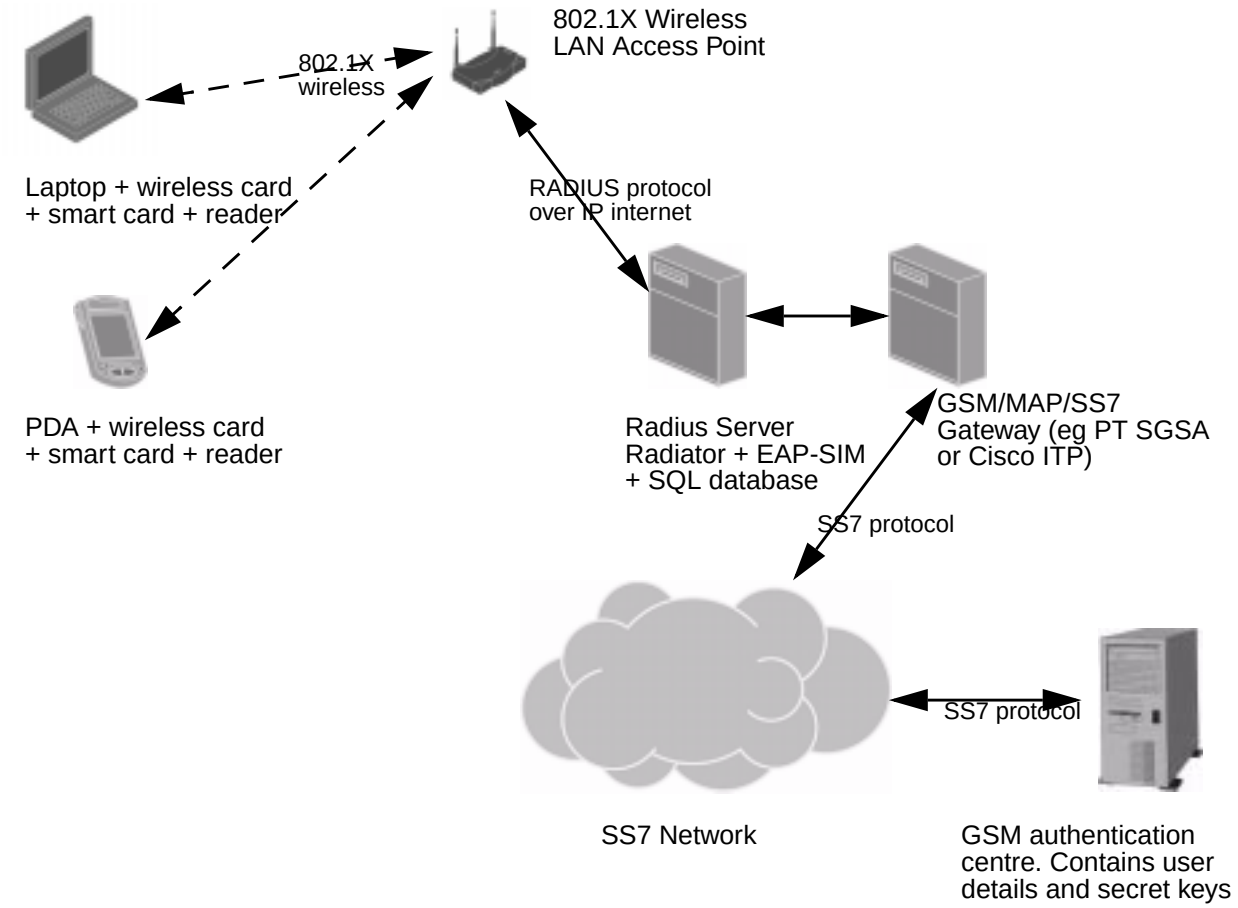
2.3 How EAP-SIM works

Typically a wireless Hot Spot or other operator has a Wireless LAN (WLAN) Access Point (AP) and access to a Radius server enabled for EAP-SIM authentication and equipped with a GSM/MAP/SS7 gateway.

A user who wants to get connected to the wireless LAN will have a computer, typically a laptop or Personal Digital Assistant (PDA) equipped with a smart-card reader, an 802.1X wireless LAN card and EAP-SIM Wireless LAN client software. The user will

insert a standard GSM SIM card, as issued by their mobile phone operator, into the smart-card reader. The SIM card could be the one from their mobile phone, or a special purpose SIM card issued by their operator. SIM cards uniquely identify a user to the GSM system, and contain the user's IMSI (International Mobile Subscriber Identity).

FIGURE 1. Typical elements of an EAP-SIM WLAN authentication system



When the user and their computer roams within range of the WLAN Access Point, the Access Point, Radius server and Wireless client software set up a communications dialog in order to authenticate the user and confirm they are allowed to access the network. During this process, the Radius server will contact the user's home GSM operator through a GSM/MAP/SS7 gateway and retrieve the GSM triplets that are used to authenticate the user.

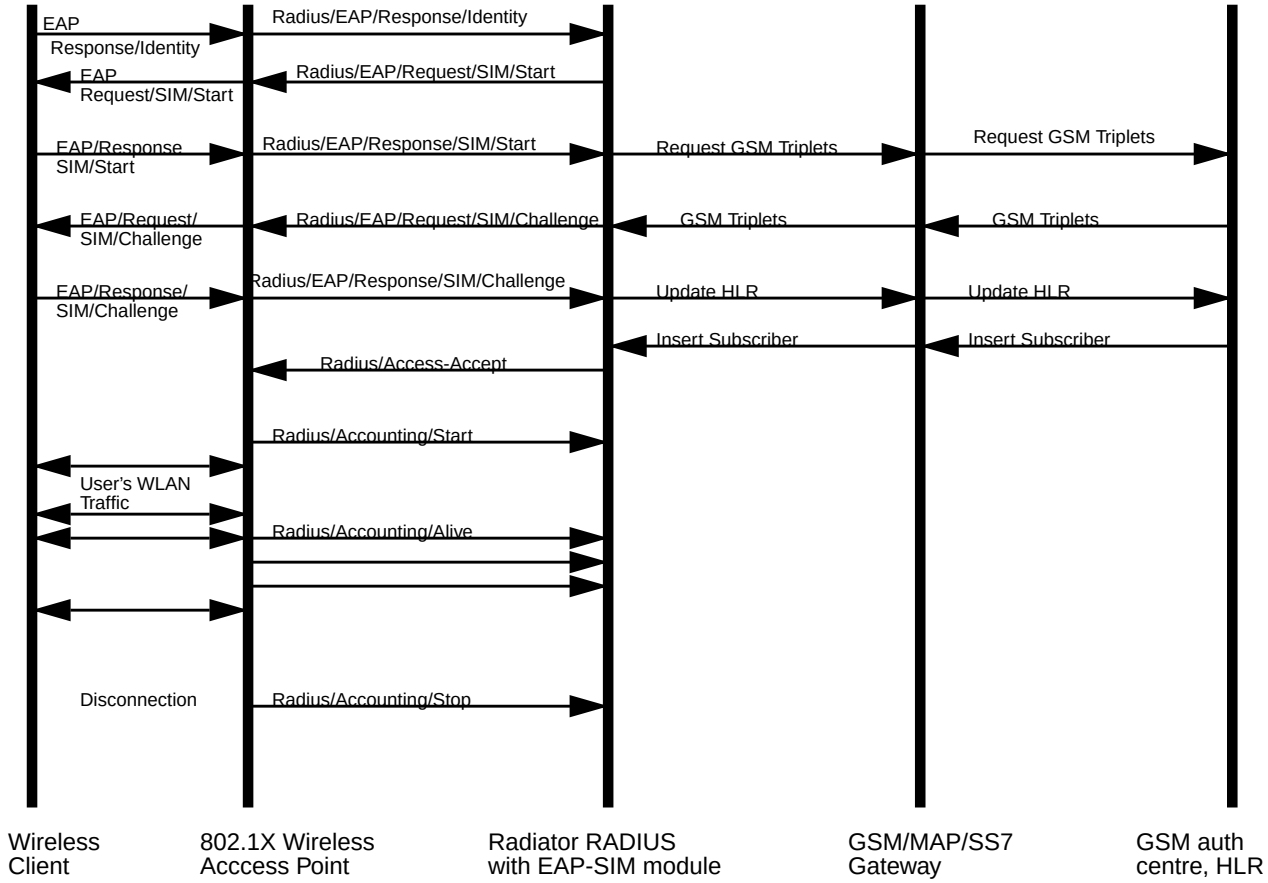
If the user's Wireless client software and SIM card is able to validate the GSM triplets correctly, the Radius server tells the AP to grant access to the WLAN. The AP connects the client computer to the WLAN, and sends some accounting information to the Radius

server, indicating that the user's wireless connection is complete. Radiator would usually be configured to insert this data into an SQL database to be used for billing.

The user will use the wireless connection to send and receive internet traffic for a period of time. During this time, the AP will typically send accounting 'Alive' messages to the Radius server, indicating the wireless session is still connected. Radiator would usually be configured to insert this data into an SQL database to be used for billing.

After a while the user will roam out of range of the AP, or turn off their client computer. The AP will then send an accounting 'Stop' message to the Radius server, indicating that the user's session is complete. Radiator would usually be configured to insert this data into an SQL database to be used for billing.

FIGURE 2. Typical messages sent during an EAP-SIM wireless session (simplified)



The overall result of this process is that only people that have a valid GSM SIM card inserted into their smart card reader will be able to get access to the Wireless LAN. Further, with proof that a valid SIM card was used, the operator is able to arrange for pay-

ment for WLAN access through the user's home GSM operator, using the existing GSM mobile phone billing infrastructure.

This simplifies the user's experience when using and paying for Wireless LAN access.

2.4 How EAP-SIM can be used

Such a system would typically be used with publicly accessible Wireless LANs hotspots such as those operated by airports, hotels, cafes, kiosks etc. The hotspot operator would install the Access Points, and the EAP-SIM equipped Radius server would be operated by a telecommunication carrier or other GSM operator.

The expectation is that users could roam in and out of range of the hotspot's APs, and the user would automatically be connected to the Wireless LAN. Later the user would be billed for the LAN usage through their mobile phone bills.

2.5 Security

These days, Wireless LAN security is a very important topic for users and operators. The main issues involve preventing access to unauthorized users, and encrypting wireless traffic with strong, hard to crack keys.

The EAP-SIM authentication standard has been developed with high standards of wireless security in mind. With EAP-SIM, passwords are never transmitted over the air or in Radius requests on the internet. EAP-SIM authentication involves secret keys and algorithms that are embedded in the SIM card and at the GSM authentication centre. The secret keys are never accessed by Radiator and are never transmitted over the air or in Radius requests on the internet. During EAP-SIM authentication, the wireless client software authenticates itself to Radiator, proving that it does indeed have access to the correct SIM card for the user. Further, the Radius server authenticates itself to the wireless client software, proving that Radiator is indeed connected to the correct GSM authentication centre.

The EAP-SIM draft standard also specifies support for dynamic Wireless Enhanced Privacy (WEP) keys, eliminating the security risks associated with fixed WEP keys. Radiator provides optional support for dynamic WEP keys in EAP-SIM authentication.

The EAP-SIM draft standard also provides support for pseudonym Temporary Mobile Subscriber Indentities (TMSI). TMSIs can be generated for each authenticating client after an initial authentication, allowing the user's real IMSI to be hidden from wireless packet sniffers. Radiator EAP-SIM includes optional support for pseudonym TMSIs.

The EAP-SIM draft standard also provides support for Reauthentication (also called fast-reconnect). This permits reauthentication of an EAP-SIM wireless client without requesting new GSM Triplets from the GSM Authentication Centre (AuC), which can result in improved reconnection performance when EAP-SIM clients roam from cell to cell. Radiator EAP-SIM includes optional support for Reauthentication.

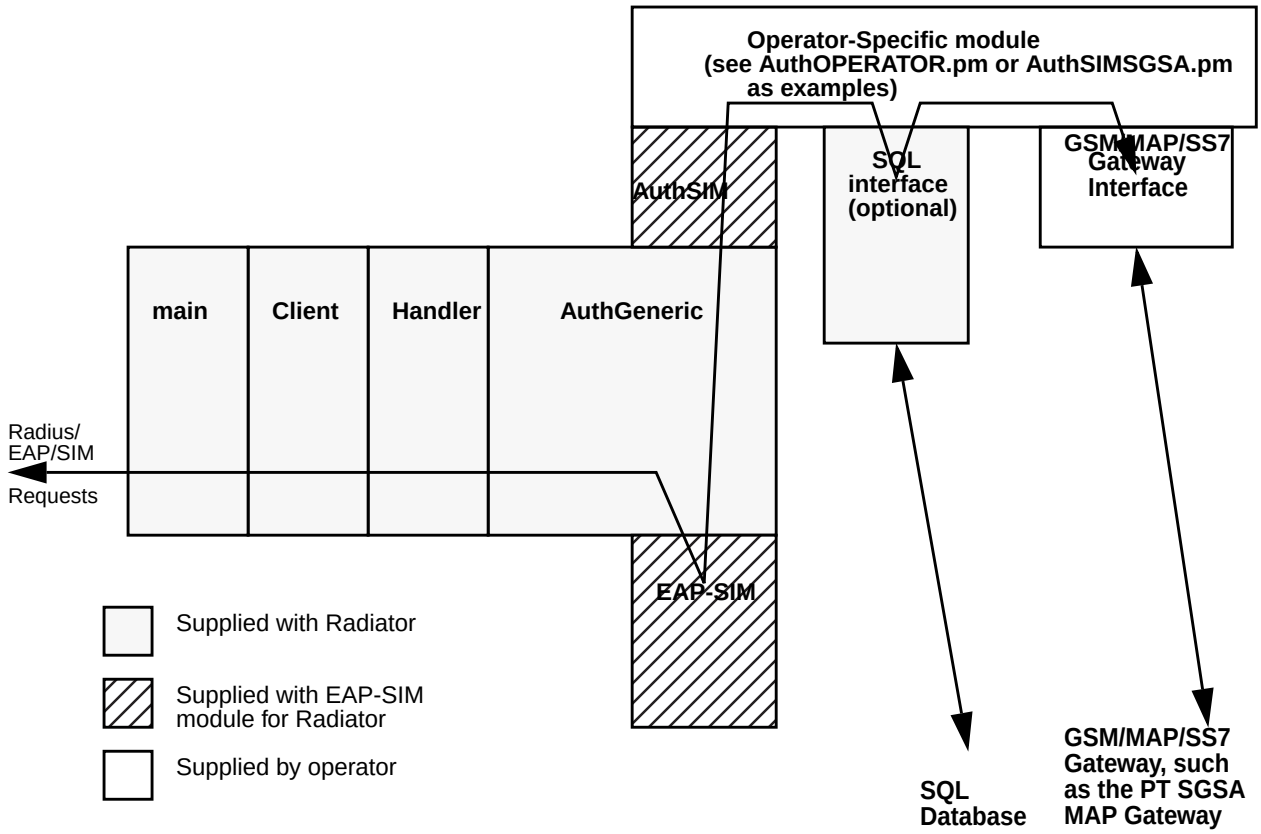
3.0 EAP-SIM support for Radiator

3.1 Architecture

Radiator Radius server is developed in a modular way to permit easy extension and enhancement. It is delivered with support for a number of EAP protocols, and a wide range of internal and external authentication methods and user databases.

In Radiator, it is simple to add support for new EAP protocols as they are developed, and it is simple to add new authentication modules (AuthBy modules) to interface with new external authentication methods. The add-on EAP-SIM support for Radiator uses both of these extension methods to add support for the low-level EAP-SIM protocol and for a generic interface to the external systems required for EAP-SIM authentication, such as an SQL database and a GSM/MAP/SS7 gateway. It also includes modules to support a direct connection to a Performance Technologies SGSA MAP Gateway.

FIGURE 3. Radiator EAP-SIM architecture



The EAP-SIM support module for Radiator is available as an optional add-on product. In order to use the EAP-SIM support module, operators are required to have a Radiator license, and also to purchase a license for the add-on EAP-SIM support module. Annual maintenance for the EAP-SIM support module is also available.

3.2 Supported EAP-SIM client software

The client software is the software that runs on the wireless PC or PDA, and which communicates with the AP to authenticate the user. For EAP-SIM authentication, special EAP-SIM wireless client software is required to be installed on the wireless computer. A number of such clients are in development or are shipping at the current time.

At the time of writing, the Radiator EAP-SIM add-on module supports the following clients:

- Microsoft Mobile 6 (www.microsoft.com)
- Cisco V5 EAP-SIM client (www.cisco.com).
- Funk EAP-SIM client (www.funk.com).
- Meetinghouse Data's AEGIS EAP-SIM client (www.mtghouse.com)
- XSupplicant EAP-SIM client for Unix, Linux, Mac etc. (www.open1x.org).
- Hostap WPA Supplicant EAP-SIM client for Unix, Linux, Mac etc. (hostap.epitest.fi).
- another proprietary EAP-SIM client, which is compliant with Haverinen version 11.

Suppliers of other EAP-SIM clients are invited to submit their client for qualification with Radiator EAP-SIM.

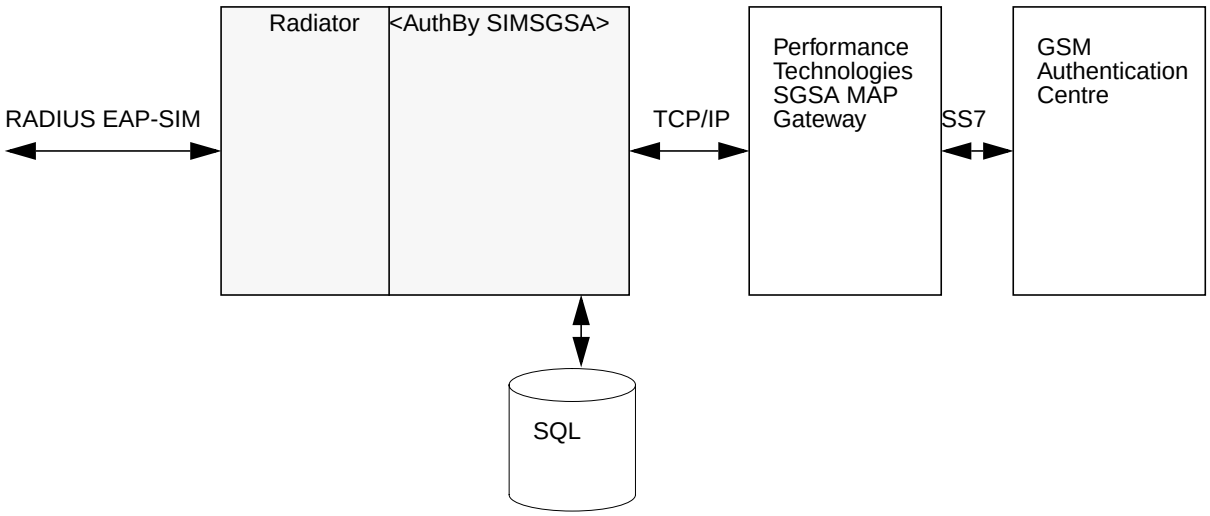
In the future, the Radiator EAP-SIM modules are expected to support all readily available EAP-SIM clients on all platforms. Purchasers of the EAP-SIM add-on module will receive updates for new wireless clients if they have purchased annual support for the EAP-SIM add-on module.

3.3 Performance Technologies SGSA MAP Gateway

Radiator EAP-SIM comes with support for the Performance Technologies SGSA MAP Gateway as a standard. This means that operators can purchase the SGSA MAP Gateway from Performance Technologies and integrate Radiator EAP-SIM without customizing or developing any other software.

The EAP-SIM module comes with a SGSA MAP Gateway simulator to permit end-to-end testing prior to the installation and commissioning of the SGSA MAP Gateway. The SGSA MAP Gateway simulator serves GSM triplets that have been previously extracted from a SIM card, allowing complete end-to-end testing, including EAP-SIM client and SIM card.

FIGURE 4. Radius-EAP-SIM architecture with PT SGSA MAP Gateway

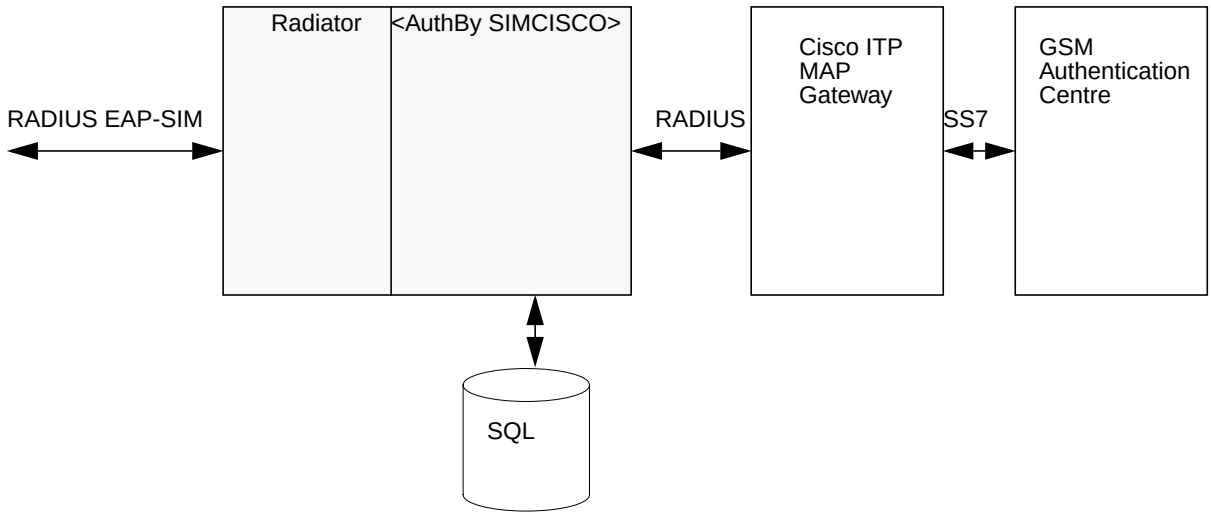


3.4 Cisco ITP MAP Gateway

Radiator EAP-SIM is also available with support for the Cisco ITP MAP gateway for qualified Cisco customers. EAP-SIM module customers who also hold a license for the Cisco ITP MAP Gateway may request and receive eadditional modules to support the-Cisco ITP MAP Gateway.

The Cisco ITP MAP Gateway provides a RADIUS based interface through which SIM authentication commands may be sent. The <AuthBy SIMCISCO> module uses this RADIUS interface to request SIM triplets from the GSM Authentication Centre.

FIGURE 5. Radius-EAP-SIM architecture with Cisco ITP MAP Gateway

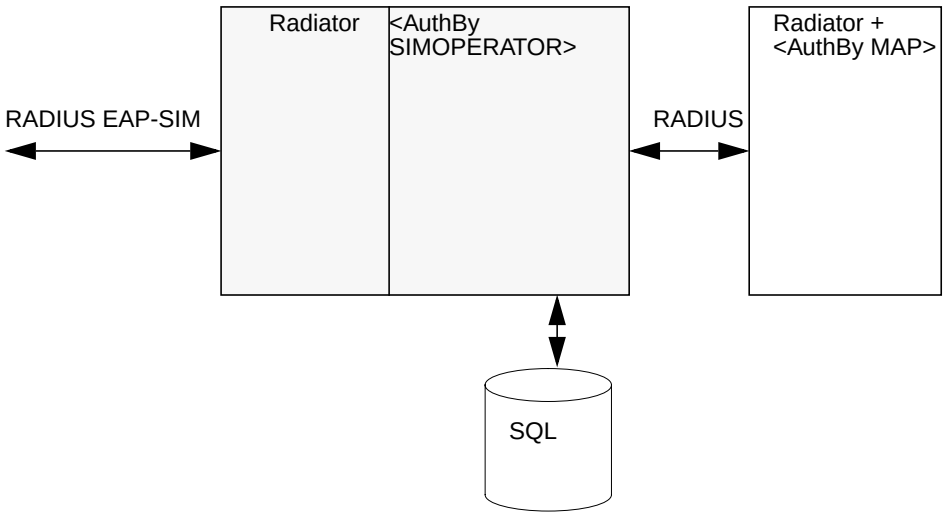


3.5 MAP Gateway Simulator

The Radius EAP-SIM module comes with a simple MAP gateway simulator that can be used for testing the Radius EAP-SIM module. It works with SIM triplets that have been previously extracted from a SIM card and stored in a flat file. During EAP-SIM authenticaiotn, the <AuthBy SIMOPERATOR> module sends RADIUS request to the MAP Gateway simulator, requesting a new set of triplets. These are extracted from the triplets file and returned to EAP-SIM.

This combination can be used to construct a complete, self contained EAP-SIM authentication system that does not rely on the GSM network for authentication. It can therfore be used for complete end-to-end testing and simulation of EAP-SIM systems.

FIGURE 6. Radius-EAP-SIM architecture with MAP Gateway simulator



3.6 Customizing

Radiator EAP-SIM comes with support for the Performance Technologies SGSA MAP Gateway as a standard. However, operators can extend and customize the EAP-SIM module to support other MAP gateways or other custom requirements.

It is expected that some EAP-SIM operators will have unique requirements for their SQL database, GSM/MAP/SS7 gateway or for their Radius accounting and billing requirements.

The Radiator EAP-SIM support has been built in a way that makes it easy to customize and modify to suit each operator's requirements. New installations of Radiator EAP-SIM may require an operator-specific module that manages and coordinates access to the SQL database and the GSM/MAP/SS7 gateway. Operators that do not wish to use the PT SGSA MAP Gateway can write and test a custom module according to their own unique requirements. Open System Consultants can provide contract assistance with this task. The operator-specific custom module is typically written entirely in Perl, but portions can be written in C or C++, and possibly other languages if necessary.

The Radiator EAP-SIM support package comes with an example operator-specific module. This example module shows how to interface to an SQL database to store and recover cached triplets with a fixed lifetime, and how to request triplets from a radius-enabled GSM/MAP/SS7 gateway. The example module (AuthSIMOPERATOR.pm) can serve as a starting point for developing an operator-specific module. The EAP-SIM package also comes with a simulator for such a radius-enabled GSM/MAP/SS7 gateway. This simulator reads GSM triplets from a data file or from a locally connected SIM card, and can be use for end-to-end testing of clients.

There is currently no standard way for handling billing, or for submitting Call Data Records (CDRs) to GSM operators. Therefore, Radiator provides methods to store EAP-SIM accounting data to an SQL database, but does not include standard software for extracting or delivering CDRs to any particular GSM operator. Any operator will be required to provide any required software for billing users, or for extracting and delivering CDRs to GSM operators.

It should be noted that the Radiator EAP-SIM module does not include an implementation of any particular GSM/MAP/SS7 gateway (it does however include a simulator for the Performance Technogies SGSA Map gateway). Such gateway software must be purchased or developed by the operator. Open System Consultants recommends the SGSA MAP Gateway from Performance Technologies. Support for the Cisco ITP MAP Gateway is also available from OSC for qualified Cisco ITP customers.

3.7 Testing

Prior to deploying a complete system, operators may wish to test the Radiator EAP-SIM module for compliance and performance.

The EAP-SIM module distribution comes with a number of tools to facilitate testing, even in an environment where there is no access to a real MAP gateway.

The Radiator SGSA MAP gateway simulator acts like the standard Performance Technologies SGSA MAP gateway. It can be used with AuthBy SIMSGSA and the sample goodies/eap_simsgsa.cfg configuration file. It gets GSM triplets from a saved data file. It does not require a connection to the SS7 network.

The Radiator Radius MAP gateway simulator receives requests for GSM triplets from the Radiator EAP-SIM SIMOPERATOR module via the Radius protocol and gets GSM triplets from a saved data file or from a locally connected SIM card. It can be used with AuthBy SIMOPERATOR example and the sample goodies/eap_simsoperator.cfg configuration file. It does not require a connection to the SS7 network.

Included is a utility for extracting triplets from a GSM SIM card and saving them to a data file that can be read by either the SGSA MAP gateway simulator or the Radius MAP gateway simulator. This means that the EAP-SIM module can be end-to-end tested with one or more EAP-SIM clients.

Evaluation versions of the EAP-SIM module and Radiator are available to suitably qualified organizations.

4.0 What about EAP-AKA?

EAP-AKA is a newly emerged EAP protocol for authenticating wireless LANs using a UMTS 3rd generation USIM card. It is described in RFC 4187. EAP-AKA' is similar and is described in RFC 5448.

The Radiator EAP-SIM module includes support for EAP-AKA and EAP-AKA' authentication, and includes sample implementations showing how to achieve complete EAP-AKA and EAP-AKA' authentication to a 3GPP Authentication Centre. EAP-AKA support has been tested against Juniper Odyssey 4.52.0.2843 and wpa_supplicant 0.6.9 through 0.7.3. EAP-AKA' suport has been tested against wpa_supplicant 0.7.3.

5.0 Further information

Installing the Radiator EAP-SIM module may require some local customizing and interface development, as well as a GSM/MAP/SS7 gateway. Open System Consultants can provide assistance with contract consulting and development. Contact info@open.com.au.

Open System Consultants can also put operators in contact with suitable prime contractors or MAP gateway suppliers, for deployment of a complete EAP-SIM solution. Contact info@open.com.au.

Various levels of pre-paid support are available from Open System Consultants, ranging from limited volume email support contracts through to 24x7 telephone support. Contact info@open.com.au for more details.

For pricing on Radiator and the EAP-SIM and EAP-AKA modules, contact info@open.com.au.

5.1 About Performance Technologies

Performance Technologies (NASDAQ NM: PTIX) develops the systems, platforms, components and software solutions for the world's evolving communications infrastructure. Their broad customer base includes companies in the communications, military and commercial markets. Serving the industry for more than 20 years, their complete line of embedded and system-level products enables equipment manufacturers and service providers to offer highly available and fully-managed systems with time-to-market, performance and cost advantages.

Performance Technologies is headquartered in Rochester, New York. Additional operational and engineering facilities are located in San Diego and San Luis Obispo, California; Norwood, Massachusetts and Ottawa, Canada. For more information, visit www.pt.com or contact sales@pt.com.