Radiator
EAP-SIM, EAP-AKA and EAP-AKA' Support

White paper discussing EAP-SIM, EAP-AKA and EAP-AKA' authentication support for Radiator.
For *Radiator SIM support* version 1.44

1.0 Introduction

This document describes the EAP-SIM, EAP-AKA and EAP-AKA' authentication standard for Wireless LANs, and outlines the support for EAP-SIM, EAP-AKA 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 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 3748 and 2869 for more details on EAP authentication for Radius. These new types of authentication are commonly used in Wireless LAN systems.

EAP-SIM is an 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.

EAP-AKA is an EAP authentication protocol, designed for use with 3GPP authentication system and USIM (Universal 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/4G/LTE mobile phone USIM card.

More recently, EAP-AKA' (AKA prime) has been introduced. It has similar properties to EAP-AKA, but with better security. The rest of this white paper uses EAP-AKA for the both unless a distinction between the two needs to be made.

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, EAP-AKA and EAP-AKA' authentication is available as an add-on package for Radiator.

The add-on package is called *Radiator SIM support* later in this white paper.

With *Radiator SIM support*, operators and carriers are able to construct complete EAP-SIM and EAP-AKA based wireless authentication and billing systems, that interoperate with and utilize the existing worldwide 2G, 3G and 4G/LTE mobile phone authentication and billing systems, enabling a simple and seamless use and billing experience for roaming wireless LAN users.

Radiator SIM support allows SIM and USIM cards to be authenticated against 2G/3G Home Location Registers/Authentication Centres (HLR/AuC) and 4G/LTE Home Subscriber Servers (HSS). Currently supported interfaces towards HRL/AuC and HSS are M3UA/SIGTRAN, Diameter Wx and Diameter SWx.

Third party MAP gateways with Wx support enable authentication against HLRs connected via SS7. Depending on operator policy, access via MAP gateway may be required for all HLR/AuC and HSS access. *Radiator SIM support* also includes source code for customizing and interfacing with other third-party MAP gateways.

2.0 What are EAP-SIM, EAP-AKA and EAP-AKA'?

2.1 Overview

EAP-SIM, EAP-AKA and EAP-AKA' are protocols for authenticating Wireless LAN access with mobile phone SIM/USIM cards and the worldwide 2G, 3G and 4G/LTE mobile phone authentication networks.

2.2 Standards

EAP-SIM is an EAP protocol for authenticating users using a 2G SIM card. It is described in RFC 4186 from the 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.

EAP-AKA is an EAP protocol for authenticating wireless LANs using UMTS 3rd generation USIM functionality. It is described in RFC 4187. EAP-AKA' ("AKA Prime") is similar and is described in RFC 5448. The Radiator EAP-AKA module is compatible with RFC 4187 and RFC 5448.

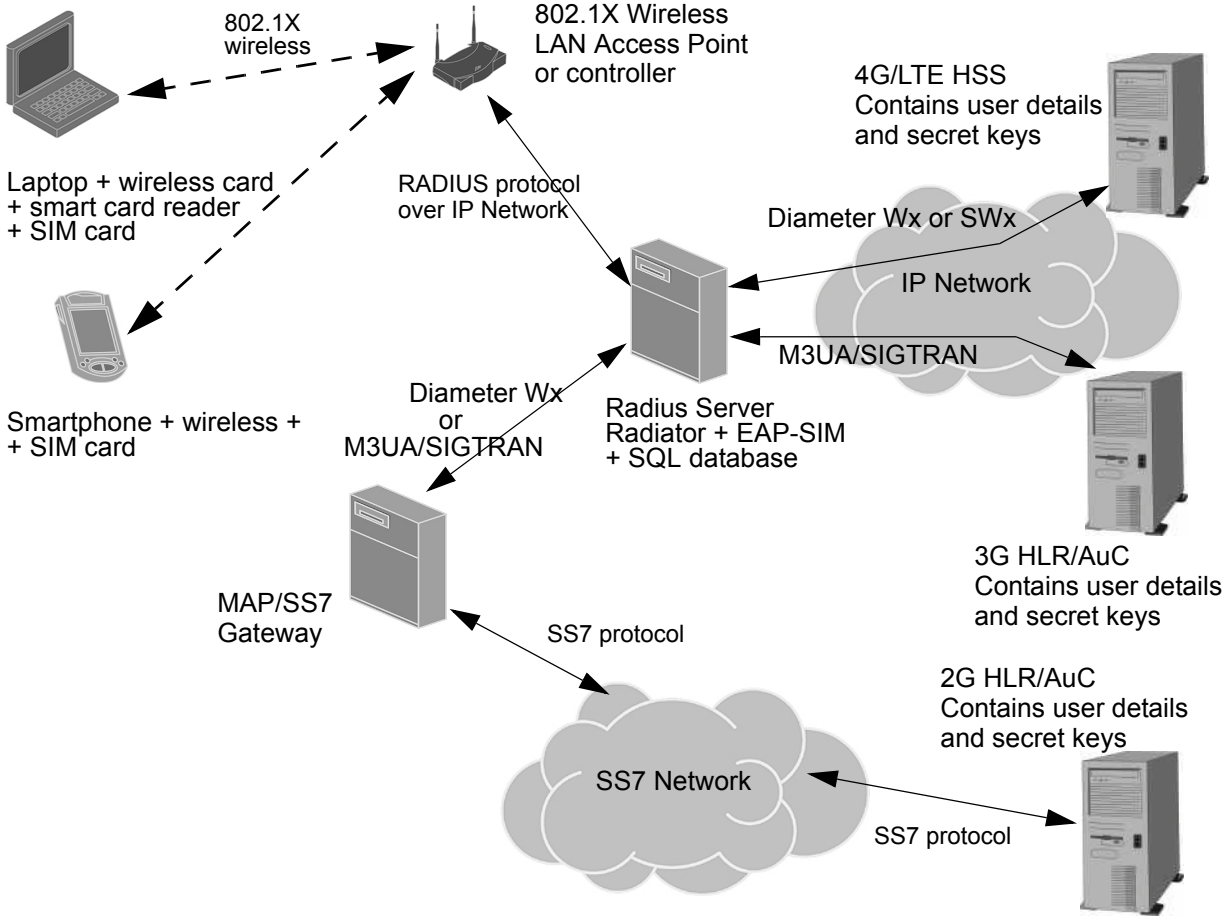
2.3 How EAP-SIM and EAP-AKA work

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 or EAP-AKA authentication. The Radius server is connected to 2G/3G/4G/LTE authentication and billing systems with Diameter Wx, SWx or M3UA/SIGTRAN interface or GSM/MAP/SS7 gateway or any combination of them.

The rest of this chapter uses EAP-SIM as an example. The functionality is practically the same for EAP-AKA and EAP-AKA'.

A user who wants to get connected to the wireless LAN will have a SIM card and a computer, typically a smartphone, tablet or laptop with a smart-card reader, and EAP-SIM Wireless LAN client software. 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. An example of an EAP-SIM and EAP-AKA WLAN authentication system



When the user 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 directly or through a GSM/MAP/SS7 gateway and retrieve the GSM triplets that are used to authenticate the user.

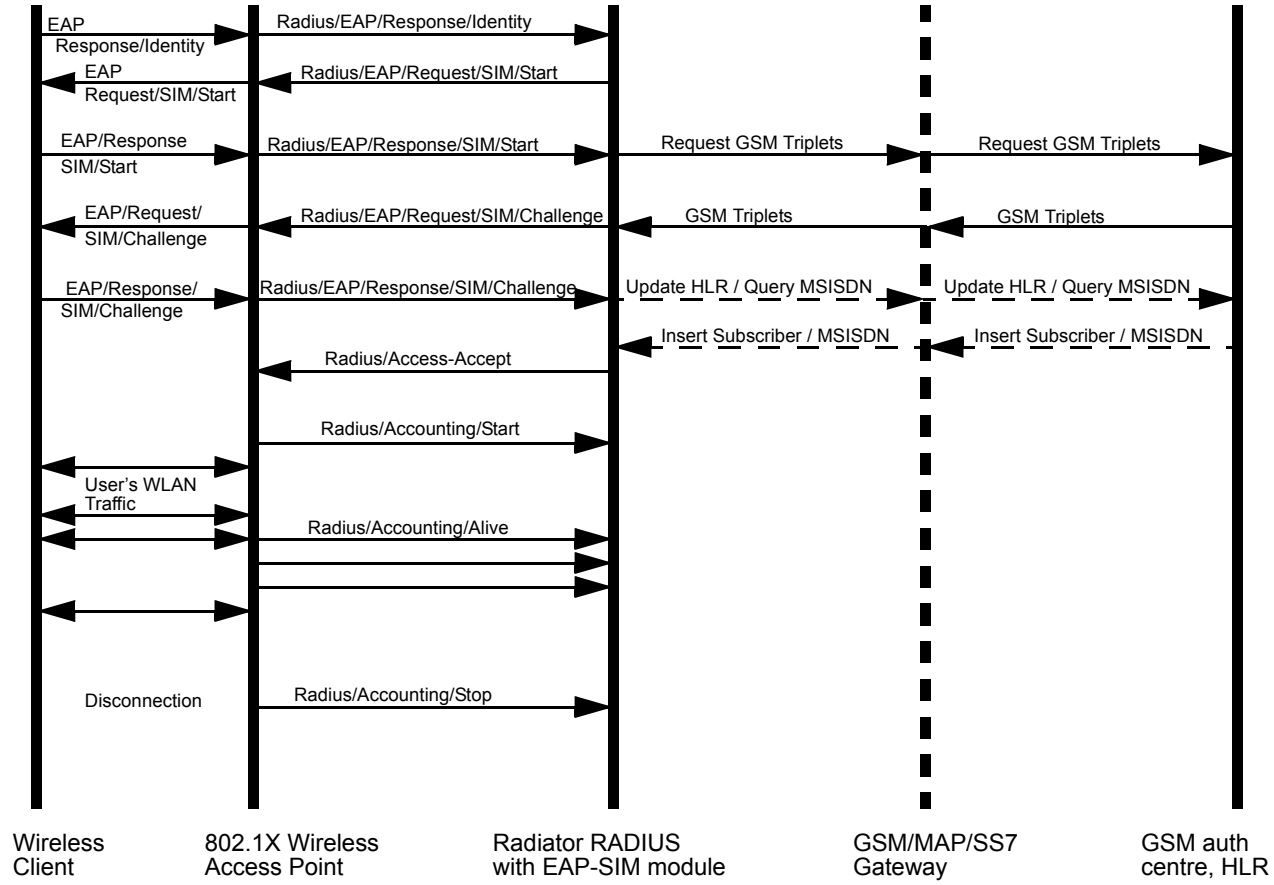
If the user's Wireless client software and SIM card is able to validate the GSM triplets correctly, the Radius server tells the AP to grant access to the WLAN. The AP connects the client computer to the WLAN, and sends some accounting information to the Radius server, indicating that the user's wireless 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 e.g., statistics or 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). Dashed lines denote optional components and messages.



The overall result of this process is that only people that have a valid SIM card 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 payment for WLAN access through the user's home mobile operator, using the existing mobile phone billing infrastructure.

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

2.4 How EAP-SIM and EAP-AKA 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 and EAP-AKA equipped Radius server would be operated by a telecommunication carrier or other mobile operator.

The expectation is that users could roam in and out of range of the hotspot's APs, and the user would automatically or as directed by Wi-Fi or other mobile offloading be connected to the Wireless LAN. Later the user would be billed for the WLAN usage through their mobile phone bill based on their plan.

2.5 Security and privacy

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

The EAP-SIM and EAP-AKA authentication protocols have been developed with high standards of wireless security in mind. No passwords are ever transmitted over the air or in Radius requests on the internet. The authentication process involves secret keys and algorithms that are embedded in the SIM/USIM card and at the 2G/3G Authentication Centre or the 4G/LTE Home Subscriber Server. The secret keys are never accessed by Radiator and are never transmitted over the air or in Radius requests on the internet. During the authentication, the wireless client software authenticates itself to Radiator, proving that it does indeed have access to the correct SIM/USIM card for the user. Further, the Radius server authenticates itself to the wireless client software, proving that Radiator is indeed connected to the correct HLR/AuC or HSS.

Both EAP-SIM and EAP-AKA support dynamic Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) keys, eliminating the security risks and management overhead of associated with fixed pre-shared keys. Radiator provides optional support for dynamic WPA-Enterprise keys in EAP-SIM and EAP-AKA authentication.

Both EAP-SIM and EAP-AKA provide support for pseudonym Temporary Mobile Subscriber Identities (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 and EAP-AKA include optional support for pseudonym TMSIs.

EAP-SIM and EAP-AKA also provide support for Reauthentication (also called fast-reconnect). This permits reauthentication of an wireless client without requesting new GSM Triplets or AKA Quintets, which can result in improved reconnection performance when EAP-SIM and EAP-AKA clients roam from cell to cell. Radiator EAP-SIM and EAP-AKA include optional support for reauthentication.

3.0 EAP-SIM and EAP-AKA support in Radiator

3.1 Architecture

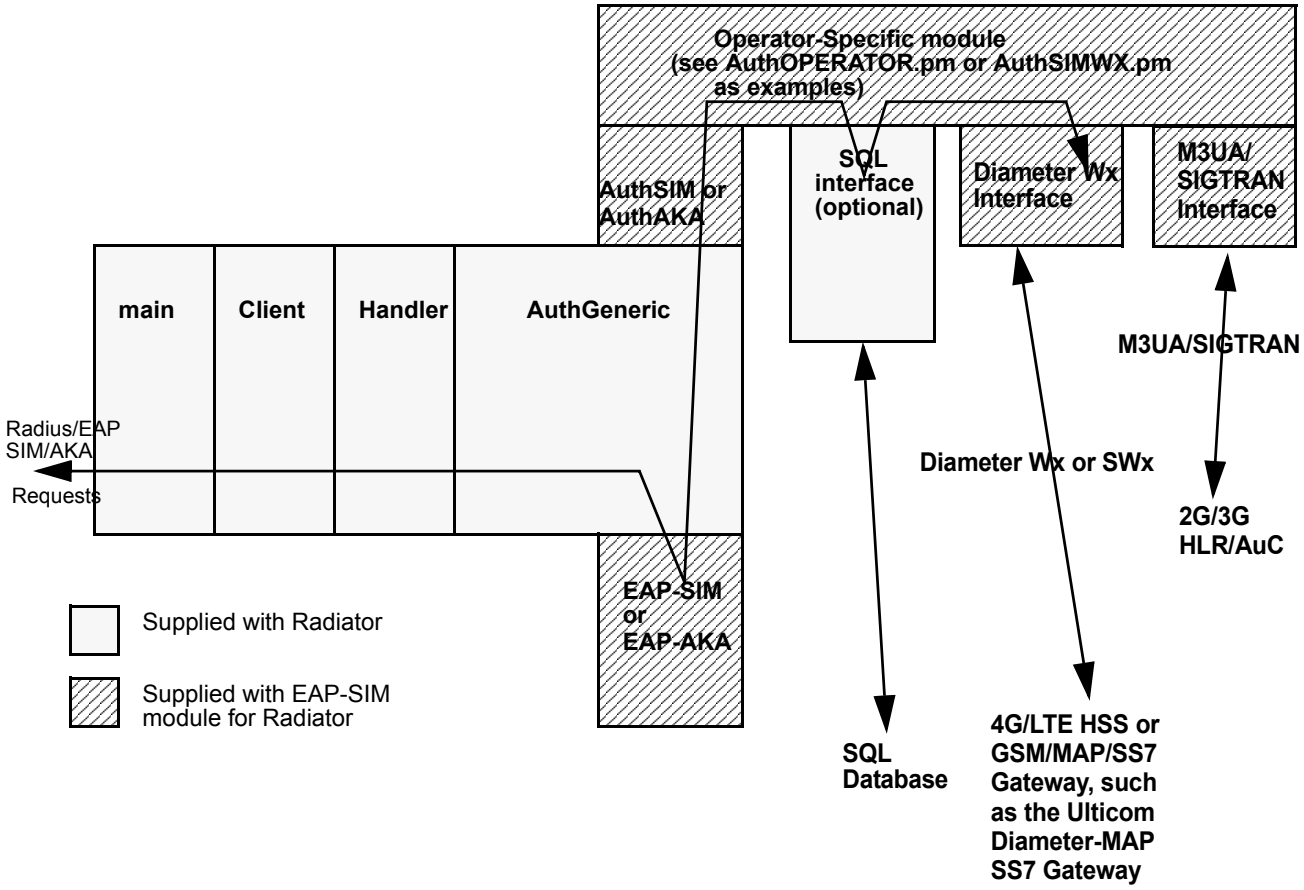
Radiator Radius server is developed in a modular way to permit easy extension and enhancement. It is delivered with support for a number of EAP protocols, and a wide range of internal and external authentication methods and user databases.

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 to interface with new external authentication methods. *Radiator SIM support* uses both of these extension methods to add support for the low-level EAP-SIM and EAP-AKA protocols and generic interfaces to the external systems required for EAP-SIM and EAP-AKA authentication, such as SQL databases, Diameter Wx and SWx interfaces and the M3UA/SIGTRAN interface.

A special feature in Radiator is the support for converting AKA authentication vectors to GSM triplets. This allows Radiator to support EAP-SIM over Diameter SWx interface. See “UMTS quintet conversion to GSM triplets” on page 9.

The M3UA/SIGTRAN, Diameter Wx and Diameter SWx interfaces are also used for connecting to MAP Gateways in order to support authenticating against SIM and USIM cards issued by an SS7 connected Authentication Centre (AuC). A gateway may also be required if the operator policy requires so.

FIGURE 3. Radiator EAP-SIM and EAP-AKA architecture



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

3.2 Supported EAP-SIM client software

The client software is the software that runs on the smartphone, table or laptop and which communicates with the AP to authenticate the user. For EAP-SIM and EAP-AKA authentication, special 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. The latest versions of major mobile operating systems already come with EAP-SIM and EAP-AKA support.

At the time of writing, *Radiator SIM support* is known to work with the following clients:

- Smartphones and tablets running Apple IOS, Blackberry, Android, Windows Phone 8, etc. where a compliant EAP-SIM or EAP-AKA supplicant is included.
- Hostap WPA Supplicant EAP-SIM and EAP-AKA supplicants for Unix, Linux, Mac etc. (w1.fi).
- Microsoft Mobile 6 (www.microsoft.com)
- Cisco V5 EAP-SIM supplicant (www.cisco.com).
- Funk EAP-SIM supplicant (www.funk.com).
- Meetinghouse Data's AEGIS EAP-SIM client (www.mtghouse.com)
- XSupplicant EAP-SIM supplicant for Unix, Linux, Mac etc. (www.open1x.org).
- another proprietary EAP-SIM supplicant, which is compliant with Haverinen version 11.

EAP-AKA support has been tested against a wide range of supplicants, including Juniper Odyssey 4.52.0.2843 and wpa_supplicant 0.6.9 through 1.0. EAP-AKA' support has been tested against wpa_supplicant 0.7.3 through 2.1. Both fast reauthentication and pseudonyms (TMSI) are supported.

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

Radiator EAP-SIM modules support all readily available EAP-SIM compliant supplicant on all platforms. Purchasers of the EAP-SIM add-on module will receive updates for new wireless supplicant if they have purchased annual support for the EAP-SIM add-on module.

3.3 UMTS quintet conversion to GSM triplets

Radiator supports optional conversion of AKA vectors to GSM triplets. This may be required, for example, when the HSS supports only SWx interface or does not return GSM triplets over M3UA/SIGTRAN interface.

When the conversion is done by Radiator, there is also no need to license additional interfaces or features on the HSS side to support EAP-SIM authentication. This simplifies HSS configuration and saves in HSS related costs.

3.4 Configuration examples

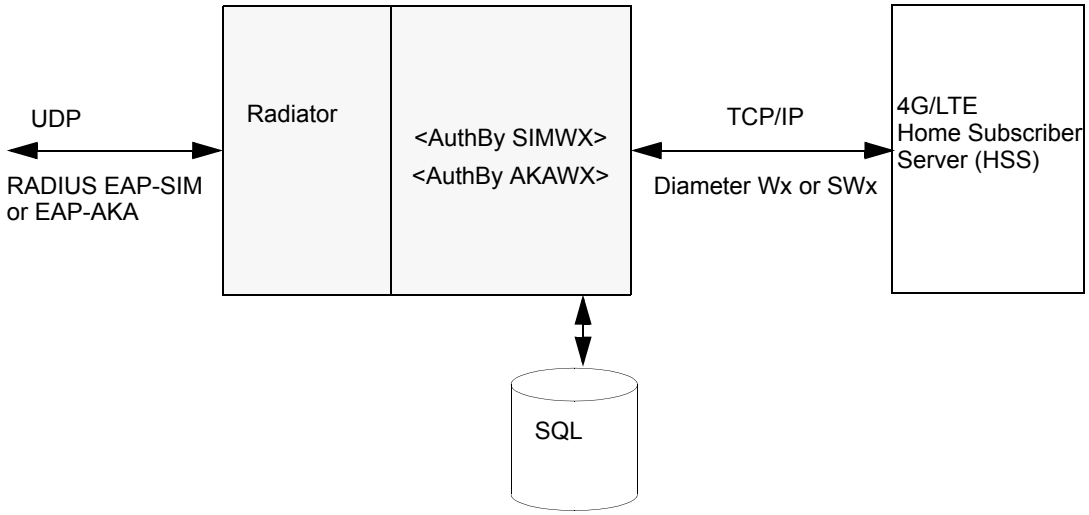
The Radiator EAP-SIM module includes configuration examples that show how to achieve complete EAP-SIM and EAP-AKA authentication with M3UA/SIGTRAN, Diameter Wx or SWx interface or Wx Diameter-MAP Gateway.

3.5 Diameter Wx or SWx interface with 4G/LTE HSS

Radiator EAP-SIM add-on module comes with support for Diameter Wx or SWx interface. With Wx interface Radiator can authenticate EAP-SIM and EAP-AKA users directly from 4G/LTE operators' Home Subscriber Server (HSS). SWx interface can not be used with EAP-SIM since the SWx interface supports EAP-AKA and EAP-AKA' only.

Note that the HSS needs to support conversion from USIM to SIM authentication vectors.

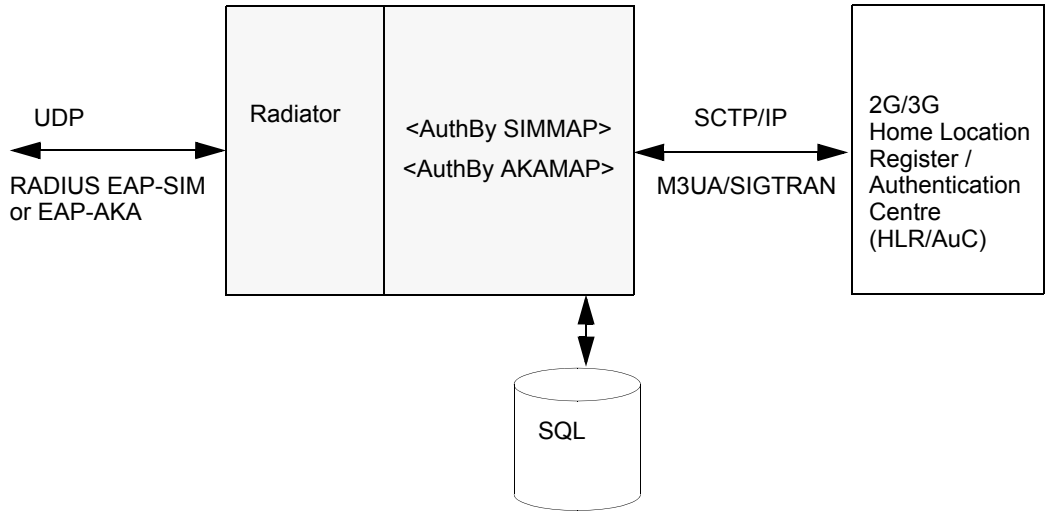
FIGURE 4. Radius-EAP-SIM and EAP-AKA architecture with Diameter Wx or SWx interface to 4G/LTE HSS



3.6 M3UA/SIGTRAN interface with 2G/3G HLR/AuC

Radiator EAP-SIM add-on module comes with support for GSM MAP M3UA/SIGTRAN interface. With M3UA/SIGTRAN interface Radiator can authenticate EAP-SIM and EAP-AKA users directly from 2G/3G operators' Home Location Register/Authentication Centre (HLR/AuC).

FIGURE 5. Radius-EAP-SIM and EAP-AKA architecture with M3UA/SIGTRAN interface to 2G/3G HLR/AuC

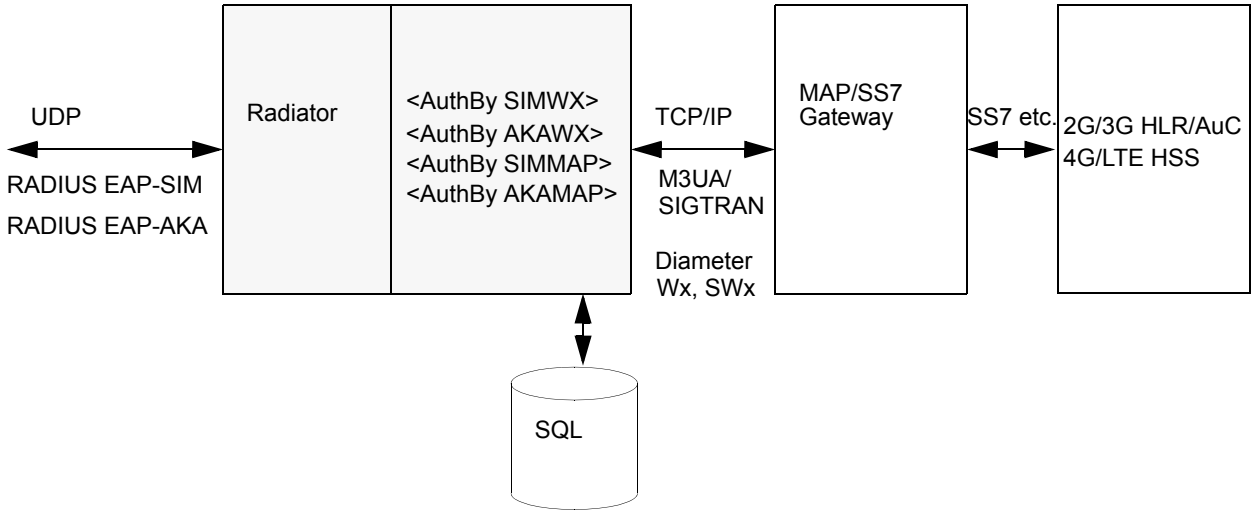


3.7 MAP/SS7 Gateway

Radiator SIM support SIGTRAN and Diameter interfaces provide a way to use MAP Gateways for integrating Radiator with SS7 networks.

After Radiator and the chosen SS7 MAP Gateway are properly installed, configured and integrated, Radiator can authenticate users directly from operators' 2G/3G HLR/AuC and 4G/LTE HSS.

FIGURE 6. Radius-EAP-SIM and EAP-AKA architecture with SIGTRAN or Diameter MAP Gateway

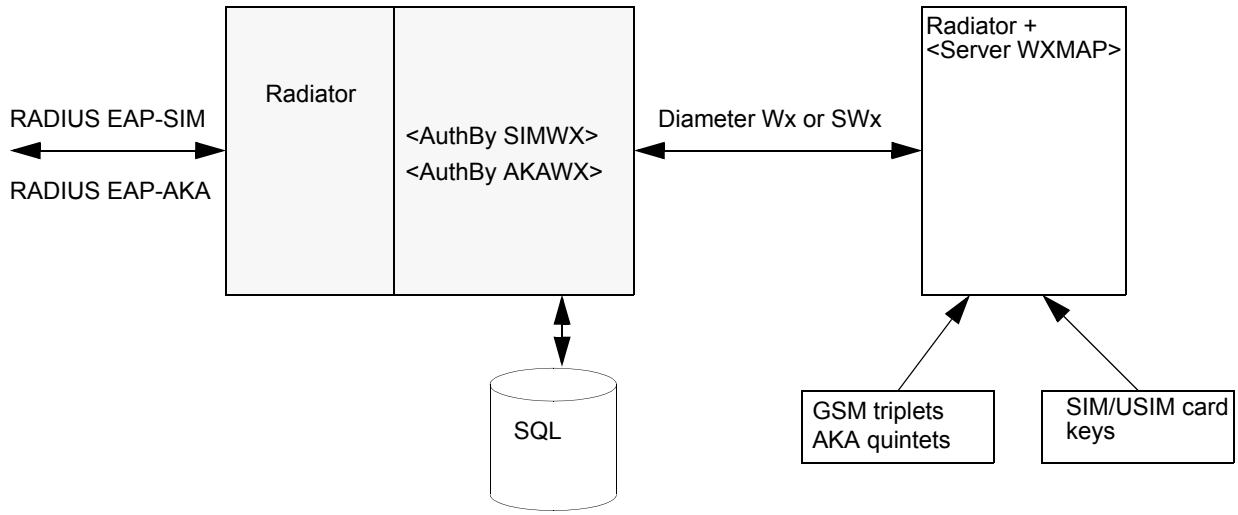


3.8 Radiator Wx/SWx server and HSS and HLR/AuC Simulator

Radiator SIM support includes a Wx and SWx server and HSS and HLR/AuC simulator to permit testing prior to the installation and commissioning of HSS or MAP Gateway. The HSS and HLR/AuC simulator supplies SIM authentication vectors that have been previously extracted from a SIM card, or SIM and AKA authentication vectors for SIM and USIM cards with known Milenage keys. This allows Supplicant, Access Point and Radiator testing without needing a real HSS or HLR/AuC.

This combination can be used to construct a complete, self contained EAP-SIM or EAP-AKA authentication system that does not rely on the operator for authentication. It can therefore be used for testing and simulation of EAP-SIM and EAP-AKA systems. It can even be used for authenticating (without the need for SS7 or a real HLR/AuC or HSS) your privately issued SIM or USIM cards.

FIGURE 7. Radius-EAP-SIM architecture with Radiator Wx/SWx server and HSS and HLR/AuC simulator

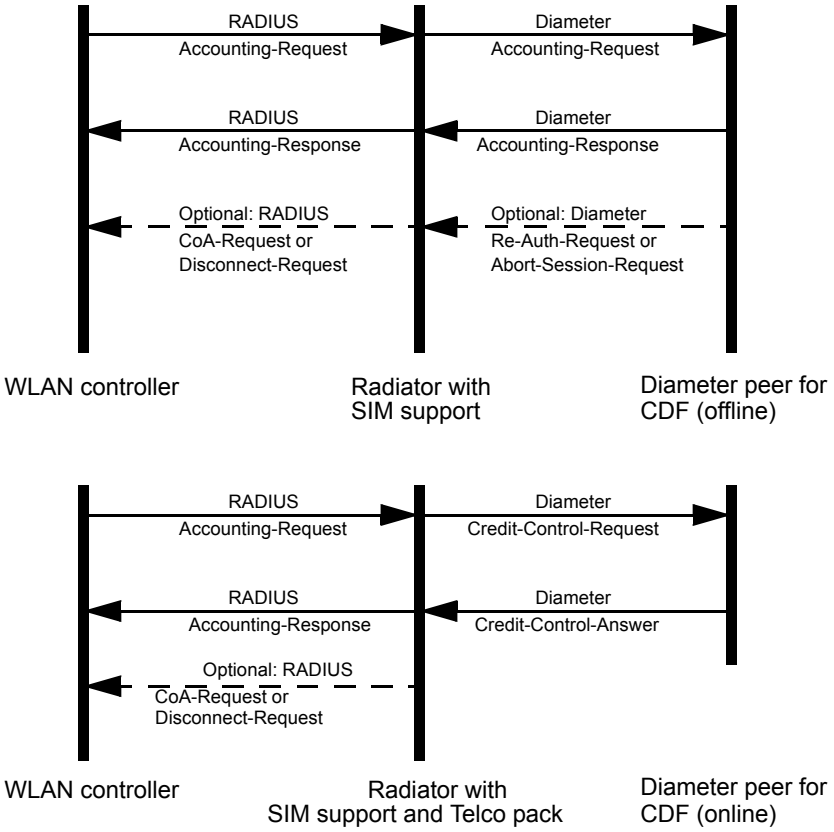


3.9 Accounting and billing over Diameter

Diameter based accounting support is supported by Radiator 4.12 and later. AuthBy DIAMETER does RFC 4005 based conversion of RADIUS Accounting requests to Diameter Accounting messages.

Radiator supports 3GPP network Charging Data Function (CDF) by converting RADIUS accounting requests to Diameter messages. Upcoming Radiator Telco pack includes online charging functions (RFC 4006 aka. DCCA and Gy).

FIGURE 8. RADIUS and Diameter accounting request flow

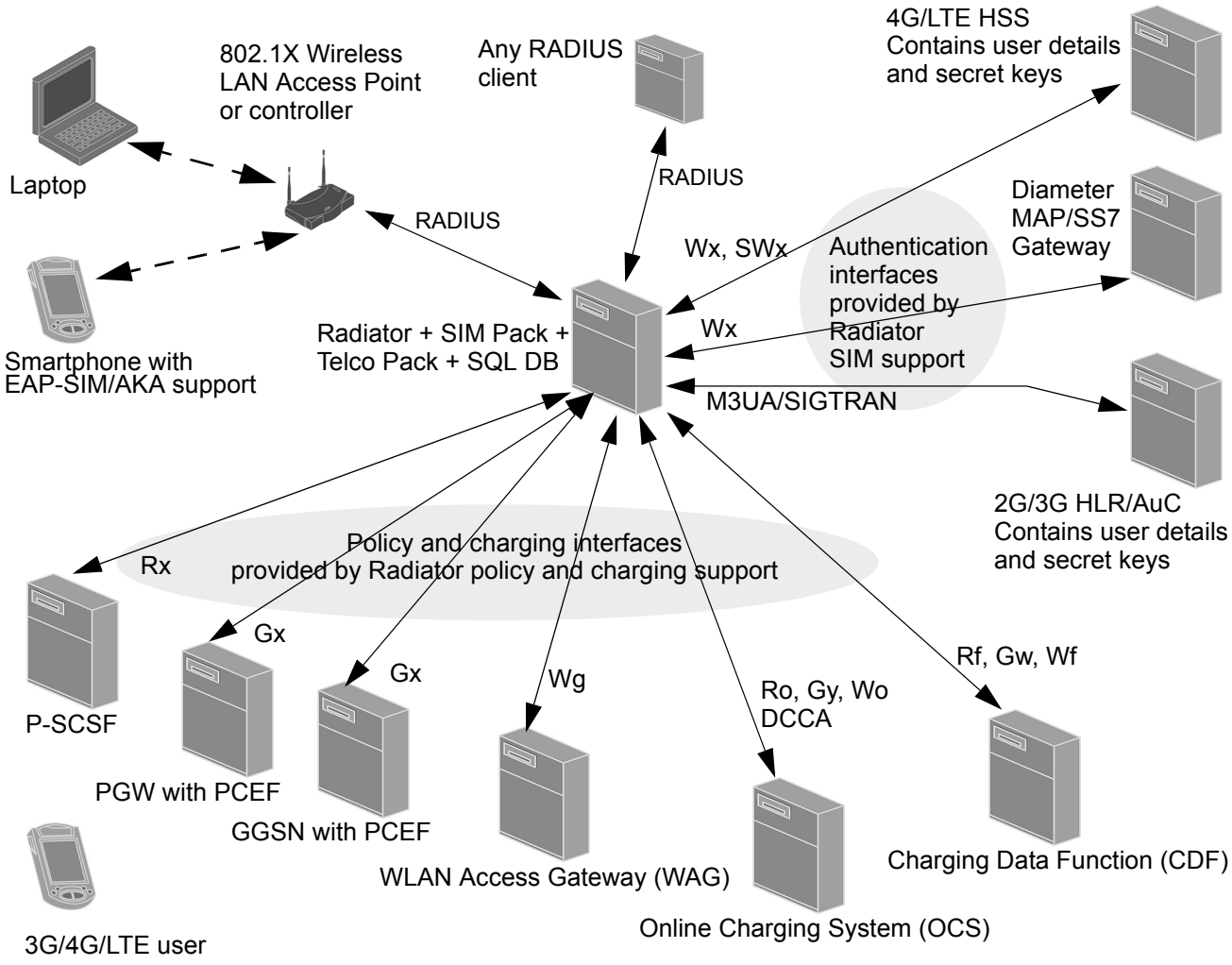


In addition to Diameter interfaces, Radiator provides methods to store accounting data to an SQL database, but does not include standard software for extracting or delivering CDRs to any particular mobile operator. Any operator will be required to provide any required software for billing users, or for extracting and delivering CDRs to mobile operators.

3.10 *Radiator SIM support* with *Radiator policy and charging support*

Radiator policy and charging support provides a number of Diameter based policy and charging interfaces. Figure 9 shows mobile oriented summary of Diameter support in Radiator. Diameter Base, NASREQ and EAP applications are not shown in the figure.

FIGURE 9. Diameter authentication, policy and charging interfaces supported by Radiator



3.11 Customizing

New installations of *Radiator SIM support* may require an operator-specific module that manages and coordinates access to the SQL database and the connection to operator's HLR/AuC or HSS. *Radiator SIM support* has been built in a way that makes it easy to customize and modify to suit each operator's requirements. Operators that do not wish to use the provided M3UA/SIGTRAN, Diameter Wx or Diameter SWx support 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.

Radiator SIM support comes with an example operator-specific EAP-SIM 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 reachable HLR/AuC. The example module (AuthSIMOPERATOR.pm) can serve as a starting point for developing an operator-specific module.

Radiator SIM support also comes with a simulator for Diameter Wx or SWx reachable HLR/AuC and HSS. This simulator reads GSM triplets and AKA quintets from a data file or from a locally connected SIM or USIM card, and can be used for end-to-end testing of clients.

It should be noted that the Radiator EAP-SIM module does not include an implementation of any particular GSM/MAP/SS7 gateway. Such gateway must be purchased or developed by the operator.

3.12 Testing

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

The EAP-SIM distribution comes with a number of tools to facilitate testing, even in an environment where there is no access to a real Diameter Wx or SWx server or MAP gateway. Open System Consultants can provide SIM/USIM cards with known secret keys. The key information can be loaded in the HSS and HLR/AuC simulator that comes with *Radiator SIM support*. The respective SIM/USIM can be installed in the tablet, phone or other device used for testing.

The Radiator Wx/SWx server and HSS and HLR/AuC simulator acts like the standard Wx and SWx Diameter server. It can be used with AuthBy SIMWX and AKAWX and the sample goodies/eap_*_wx.cfg configuration files. It gets GSM triplets from a saved data file, or GSM triplets and AKA quintets from a SIM or USIM card Milenage key file. It does not require a real Diameter Wx or SWx server or a connection to a SIGTRAN or 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 the Radiator HSS and HLR/AuC simulator. This means that the EAP-SIM and EAP-AKA modules can be end-to-end tested with one or more EAP-SIM or EAP-AKA supplicants, using either real or simulated SIM or USIM cards.

Evaluation versions of the *Radiator SIM support*, and Radiator with SIM/USIM cards are available to suitably qualified organizations.

4.0 Further information

Open System Consultants can provide a range of design, installation, configuration, testing, commissioning and support services. Contact info@open.com.au.

Open System Consultants can also put operators in contact with suitable prime contractors for deployment of a complete EAP-SIM/EAP-AKA 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, *Radiator SIM support* and *Radiator policy and charging support* contact info@open.com.au.

http://www.open.com.au