

Steel-Belted Radius SIM Server AAA Platform for GSM and UMTS Operators

The Juniper Networks Steel-Belted Radius (SBR) SIM Server Authentication, Authorization and Accounting (AAA) platform enables service providers to deliver new IP-based services to mobile customers – including access over a wireless local area network (WLAN) and in Unlicensed Mobile Access (UMA) / Generic Access Network (GAN) environments – while leveraging installed infrastructure to keep capital expenditures and operational changes to a minimum. The SBR SIM Server also gives service providers the ability to extend their current mobile voice and data offerings through femtocells.

The SBR SIM Server builds on proven Steel-Belted Radius technology used in 9 of the world's top 10 mobile carriers. It is integrated into Juniper's Session Resource Control portfolio of policy management products, which manage the user service experience and control Juniper's end-to-end infrastructure portfolio.

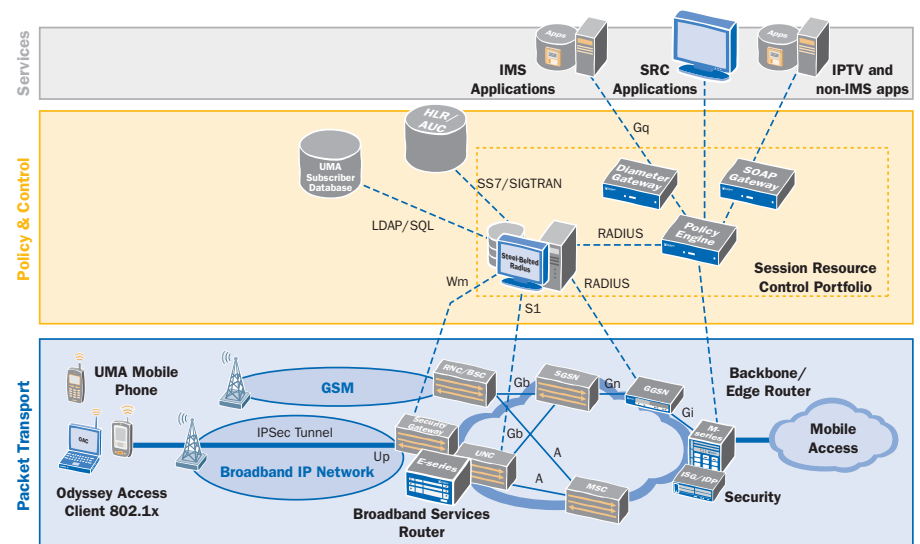
Product Description

The Juniper Networks Steel-Belted Radius SIM Server AAA platform enables service providers to deliver IP-based data and voice services, such as dual-mode phone and secure hotspot access, using existing mobile infrastructure including existing Home Location Register (HLR), billing platforms, and customer care systems.

The SBR SIM Server supports user authentication in multiple deployment scenarios:

- Unlicensed Mobile Access (UMA) / Generic Access Network (GAN) environments.** Extends mobile voice and data services over an IP access network. Allows seamless roaming and handover between wireless networks like Wi-Fi® and Bluetooth® or GSM and UMTS using the same dual-mode mobile phone. This network architecture enables mobile operators to deliver voice, data, and IMS / SIP (IP Multimedia Subsystem / Session Initiation Protocol)-type applications to mobile phones attached to local IP networks, thus expanding service offerings and revenue growth. This is the first step in the convergence of mobile, fixed, and Internet telephony (otherwise known as Fixed Mobile Convergence).
- Secure 802.1x hotspots.** Enabled using Extensible Authentication Protocol (EAP)-SIM or EAP-Authentication and Key Agreement (AKA) user authentication methods, which leverage existing SIM-based authentication mechanisms and roaming relationships to enable customers and roaming partners to use a single identity (SIM) across all access methods and services. The SBR SIM Server is integrated into the network and ties the service provider customer base to the service offering. This enables a seamless experience across access methods with unified billing. In further support of secure hotspot access, Juniper also provides the Odyssey Access Client solution to perform the user supplicant function in 802.1x authentication.
- Secure open hotspots.** For operators who have not yet adopted 802.1X, SBR SIM Server can be leveraged to authenticate hotspot users to the network and deliver services based on out-of-band delivery of a secure one-time password via the Short Message Service (SMS) text messaging protocol. Again, billing integration is provided through RADIUS accounting and Call Detail Record (CDR) generation to enable unified billing.

SBR SIM Server integrates with UMA network controllers (UNC) and Security Gateways (or packet data gateways) in UMA / GAN deployments to identify and differentiate traffic and authenticate users with the appropriate back-end.



- **Next-Generation Networks (NGNs).** SBR SIM Server facilitates the migration to a converged IP NGN by supporting SS7 and SIGTRAN (SS7 over IP) for HLR communication, enabling operators to seamlessly transition to next-generation IP-based signaling networks.

Features and Benefits

Enables Operators to Offer New High-performance Mobile Services over IP

Juniper Networks SBR SIM Server enables service providers to offer new, high-performance mobile voice and data services over wireless IP access networks, facilitating roaming and seamless handover between networks by enabling the same mobile identity on unlicensed wireless networks as on the mobile network. The SBR SIM Server provides an interface for passing subscriber credentials from the IP network to the SIM-based authentication information stored in the HLR / Authentication Center (AuC) over an SS7- or SIGTRAN-based network. Users gain IP network access based on the successful authentication of SIM credentials passed from their mobile devices against the HLR / AuC. In this scenario, the SBR SIM Server performs the following functions:

- Provides a bridge between the RADIUS / IP-based public WLAN infrastructure and the SIM-based subscriber management system used in the mobile network infrastructure
- Authenticates SIM-based user credentials over the WLAN RADIUS / IP network against operator HLR / AuC
- Supports authorization against service profiles stored in the HLR, SQL/Lightweight Directory Access Protocol (LDAP) databases so that operators can deliver differentiated services to their WLAN customers
- Sends RADIUS accounting streams or CDRs to the operator billing system, integrating the billing with the existing operator infrastructure
- Sets up a secure, encrypted connection over the wireless link, protecting data privacy for the end user

Service Delivery in a UMA or 802.1X Environment

Many GSM and UMTS operators are implementing UMA or 802.1X-based services. This allows them to offer secure hotspot access or leverage their mobile voice and data services over a WLAN, in both cases leveraging existing roaming relationships. In these environments, SBR SIM Server lets operators authenticate subscribers via EAP-SIM and EAP-AKA, offering a unified user experience.

EAP-SIM Authentication

The EAP-SIM protocol specifies enhancements to GSM authentication and key agreement which provide message integrity protection along with mutual authentication.

EAP-AKA Authentication

The Third-Generation Partnership Project (3GPP) has specified an improved Authentication and Key Agreement (AKA) for use in UMTS networks. EAP-AKA provides greater security through the use of longer session keys and replay protection.

UMA Authentication

In UMA environments, SBR SIM performs all AAA functions, authenticating users to the network, authorizing their connections,

and writing RADIUS accounting and CDRs. It also integrates with existing UMA network controllers (UNC) and security gateways or packet data gateways to ensure compatibility in the network environment.

Steel-Belted RADIUS SIM Server was developed with a modular architecture using both EAP-SIM and EAP-AKA plug-in modules to manage the appropriate authentication requests from subscribers. These modules support user authentication based on International Mobile Subscriber Identity (IMSI) information or anonymous authentication based on pseudonym values, as well as re-authentication, so that carriers can regularly replace the encryption keys used over the wireless link to protect the privacy of user data.

Data Security

In an 802.1X hotspot environment, once a subscriber is granted access to the network, the subscriber's wireless connection is encrypted using the Wi-Fi Protected Access™ 2 (WPA2) or WPA protocol, enabling dynamic Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP) or Wired Equivalent Privacy (WEP) protocol encryption algorithms, depending on which protocol(s) the subscriber's 802.1X access client supports. These encryption protocols protect session data against wireless eavesdropping to maintain data privacy within the hotspot.

Odyssey Access Client

For secure hotspot access, an EAP-SIM or EAP-AKA-compatible 802.1X supplicant is a necessary component of the SBR SIM solution. Juniper Networks Odyssey Access Client (OAC) is an ideal choice for this key component. To provide a simple user interface and ensure a positive user experience, OAC runs on Microsoft® Windows XP, 2000, 98, Me, Pocket PC 2002, and Windows Mobile® 2003/2005. It supports any 802.1X-compatible wireless adapter card for compatibility with the widest range of user devices. It also supports a wide range of WLAN protocols including EAP-TTLS, EAP-PEAP, EAP-TLS, and Cisco's EAP-FAST and LEAP, to support any network and security requirement. In addition, the Juniper Networks Odyssey Access Client supports all popular encryption protocols, including WPA2 and WPA.

Service Delivery in an Open Hotspot Environment

As an interim step to complete deployment of 802.1X-based secure hotspot services, or to more securely handle non-802.1X users, carriers can implement a hybrid approach that relies on out-of-band delivery of login credentials via the SMS text messaging protocol.

SMS One-Time Password

The one-time password via SMS solution is supported through the SMS authentication plug-in, an optional, license-enabled component of SBR SIM. In this model, a temporary account is created for the subscriber and the account's temporary one-time password (OTP) is transmitted securely to the user's device using SMS. The SMS message may be composed in the language of choice of the subscriber. This solution requires that subscribers have the following equipment:

- A mobile device capable of receiving SMS messages
- A wireless client, such as a laptop or a PDA with an 802.11 wireless network adapter card
- A browser

This method offers the following advantages:

- It lets carriers offer WLAN access based on information in existing mobile subscriber databases (HLR / AuC)
- It uses a common delivery mechanism that may already be employed in support of other services – that of delivering confirming information to users' mobile phones
- It minimizes the possibility of fraud by delivering login information to a user's phone, making it more likely that the owner of the account is the one accessing the network
- It doesn't require upgrading infrastructure to 802.1X, nor does it require client software on the wireless device
- In the absence of 802.1X-enabled hotspots and / or 802.1X-capable devices, this solution provides a means for GSM subscribers to gain access to secure Wi-Fi networks, still enabling unified billing

Authorization / Service Levels

In addition to authenticating Universal SIM (USIM)-based users to the hotspot and setting up their secure connections, SBR SIM lets carriers authorize subscriber connections according to profile information provisioned in the HLR, SQL / LDAP databases.

Using information stored in the HLR database, such as bearer service, teleservice, and operator-defined call barring (ODCB), SBR SIM can determine whether the subscriber is authorized for such access and grant or deny access to the network. It is also possible to utilize further authorization data from an SQL- or LDAP-based user provisioning system.

Accounting Data and Billing Services

SBR SIM supports both RADIUS accounting and CDRs for use in customer billing. The RADIUS accounting information received from access points, access controllers or security gateways is recorded and has multiple options for use. It can be stored locally, stored in an SQL database, or forwarded by SBR SIM to other billing platforms or mediation systems, thus providing the GSM operator with a flexible array of billing options.

Additionally, specific pieces of information contained within the RADIUS accounting flow, which are relevant to specific services and their associated billing requirements, can be extracted from RADIUS accounting streams and included within XML-configurable CDRs, which SBR SIM will transmit directly to the mediation or billing system.

Performance

SBR SIM is a proven solution used in many of today's top mobile networks and ready to scale to meet the growth of service provider services. SBR SIM Server's robust performance makes it capable of handling the busiest networks by offering several methods for scaling the solution. Authentication and accounting services leverage server resources for processing, thus enabling easy expansion in processing speeds through additional server resources or additional platforms.

Further solution scaling is achievable by offering flexible options to expand throughput across the telephony network. This can be accomplished by increasing the number of licensed SS7 links or transitioning to the IP based SIGTRAN protocol.

SIGTRAN Support

The growth of 2.5G and 3G wireless technologies, as well as the convergence of voice with data networks and services, has led to the convergence of signaling, data, and voice networks to an all-IP backbone. SBR SIM server integrates into this all-IP signaling network by supporting SIGTRAN (SS7 over IP).

SIGTRAN, a working group of the IETF, has defined a protocol for the transport of real-time signaling data over IP networks. The SBR SIM solution supports SS7 messaging over IP (SS7oIP) via SIGTRAN, a new transport layer which leverages Stream Control Transmission Protocol (SCTP).

| Feature | Benefits |
|--|---|
| Proven reliability and scalability | <ul style="list-style-type: none"> • Full-function RADIUS / AAA server manages authentication, authorization, accounting and service delivery on GSM and UMTS networks. • Reliably handles even the busiest networks. |
| Easily integrated into existing mobile infrastructure | <ul style="list-style-type: none"> • Enables operators to tap into new revenue opportunities. • Gives operators ability to offer IP-based services to customers without upgrading the customer care infrastructure. • Allows operators to extend services into unlicensed radio networks such as Wi-Fi and Bluetooth. • Gives operators the ability to authorize customers for specific services based on existing HLR / AuC profiles. |
| Works in 802.1X, non-802.1X, UMA / GAN, and femtocell environments | <ul style="list-style-type: none"> • Flexible authentication options permit subscriber authentication via EAP-SIM, EAP-AKA, or one-time password (via SMS). • Enables operators to leverage existing SIM or SMS infrastructure to facilitate secure subscriber provisioning, authentication, and billing. • Lays a trusted foundation for UMA voice and data services and Fixed Mobile Convergence based on the IP Multimedia Subsystem (IMS) as RADIUS migrates to DIAMETER. • Integrates seamlessly into next-generation IP-based signaling networks. |

Product Options

Secure Hotspot Access with EAP-SIM / AKA or UMA Network Deployment

SBR SIM Server runs on Sun Solaris Server with a PCI, cPCI, or PMC bus architecture. The base configuration of SBR SIM Server includes one T1 / E1 interface card licensed for two 64k links for SS7 configurations, or a minimum configuration of 2 associations when using a SIGTRAN configuration.

Secure Hotspot Access with SMS

SBR SIM Server with SMS Module runs on Sun Solaris Server with a PCI, cPCI, or PMC bus architecture. The base configuration of SBR SIM Server includes one T1 / E1 interface card licensed for two 64k links for SS7 configurations, or a minimum configuration of 2 associations when using a SIGTRAN configuration.

Product Requirements

- Sun server running the Solaris™ 9 Operating System
- For secure hotspot access based on 802.1X and EAP-SIM or EAP-AKA user authentication, the solution also requires that an EAP-SIM- or EAP-AKA-compatible 802.1X supplicant such as Juniper Networks Odyssey® Access Client be running on the subscriber's mobile device, and that 802.1X-compliant access points be installed at the hotspot.

Ordering Information for Steel-Belted Radius SIM Server

SBR SIM Server combines leading technologies from Juniper Networks and Ulticom and is comprised of the following components:

- Juniper Networks Steel-Belted Radius Service Provider Edition RADIUS Server with EAP-SIM, EAP-AKA, and optional SMS plug-in modules.
- Ulticom's Signalware SS7 signaling software and E1 / T1 interface card, licensed for up to 64 links, or SIGTRAN signaling over IP.

The following part numbers represent the most commonly ordered SBR SIM Server products. Contact your Juniper sales representative for a full list of available products and their pricing information.

| Part Number | Description |
|----------------|---|
| SBR-SIMAKA-IC | Supports SIM/AKA SS7 Interface - Solaris (1000 concurrent user/2 SS7 links license) Includes SS7 interface card |
| SBR-SMS-IC | Supports SMS SS7 Interface - Solaris (1000 concurrent user/2 SS7 links license) Includes SS7 interface card |
| SBR-SIMAKA-SIG | Supports SIM/AKA SIGTRAN Interface - Solaris |

About Juniper

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support many different services and applications at scale. Service providers, enterprises, governments, and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security, and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at www.juniper.net.



CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100

www.juniper.net

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, 25/F
ICBC Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS

Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Addlestone
Surrey, KT15 2PG, U.K.
Phone: 44-(0)-1372-385500
Fax: 44-(0)-1372-385501

Copyright © 2007, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.