



INTRODUCTION TO IMSI PRIVACY PROTECTION FOR WI-FI WITH RADIATOR SIM PACK

WHITEPAPER OCTOBER 2024

CONTENTS	PAGE
Introduction	2
Overview of Wi-Fi SIM-based authentication	3
Security issues with SIM-based authentication in Wi-Fi networks	3
Drivers for secure Wi-Fi SIM-based authentication	4
The solution is IMSI Privacy Protection for Wi-Fi	5
Customer case	6
About the Radiator SIM Pack	7
About Radiator Software	8
Contact details	8

INTRODUCTION

One of the key use cases for SIM-based authentication, Wi-Fi offloading enables SIM-based devices to automatically switch data and voice traffic from mobile networks to Wi-Fi networks. This lets mobile carriers and operators reduce their operating costs, and provide better network coverage and customer service, in locations with high amounts of mobile traffic. However, without IMSI Privacy Protection for Wi-Fi the mobile user's identity will be exposed on the Wi-Fi network when the device is authenticated and the latest Android and iOS mobile devices will also give the user a security warning and may refuse to connect automatically.

Since Wi-Fi offloading, Voice over Wi-Fi and Wi-Fi roaming capabilities are growing in importance, mobile OS manufacturers are putting pressure on the industry to improve Wi-Fi security, leading to a clear need for reliable IMSI Privacy Protection.

This white paper gives an overview of the security issues with Wi-Fi SIM-based device authentication and introduces the Radiator SIM Pack, which is a proven solution for IMSI Privacy Protection for Wi-Fi.

WHICH BUSINESSES CAN BENEFIT FROM IMSI PRIVACY PROTECTION FOR WI-FI?

IMSI Privacy Protection for Wi-Fi brings benefits to companies that provide mobile connections and to companies that own or operate Wi-Fi networks.

THESE INCLUDE:

- Mobile carriers and network operators
- Commercial enterprises and venues that provide Wi-Fi services
- Public organisations with extensive Wi-Fi networks, like city authorities
- Companies that sell Wi-Fi network capabilities
- Public transport companies with their own Wi-Fi networks, such as airlines and underground metros

WHAT IS IMSI?

In SIM-based mobile devices, like smart phones and tablets, the user's unique identifier is stored on the SIM card in a standard format known as the International Mobile Subscriber Identifier, or IMSI for short.

OVERVIEW OF WI-FI SIM-BASED AUTHENTICATION

Modern SIM-based devices, like smartphones and tablets, are able to join and switch between different networks automatically. This is especially valuable to mobile operators who want to offload data from their mobile network to a nearby Wi-Fi network, because Wi-Fi connections are significantly cheaper to operate. It also enables Wi-Fi providers to monetize their Wi-Fi networks and provide services in partnership with mobile operators.

Wi-Fi SIM-based authentication is essential to making these capabilities work. Before a device is allowed to join a new Wi-Fi network, it must be authenticated using the IMSI. For this reason, Wi-Fi SIM-based authentication is supported by the latest Android and iOS mobile devices. However, there are still some security issues with this type of authentication. As a result, mobile OS manufacturers are now pushing for even better security on Wi-Fi networks and they require IMSI Privacy Protection with all new OS versions.

The Radiator SIM Pack is the best way for mobile operators and Wi-Fi providers to add IMSI Privacy Protection and improve the security of SIM-based authentication on their Wi-Fi networks.

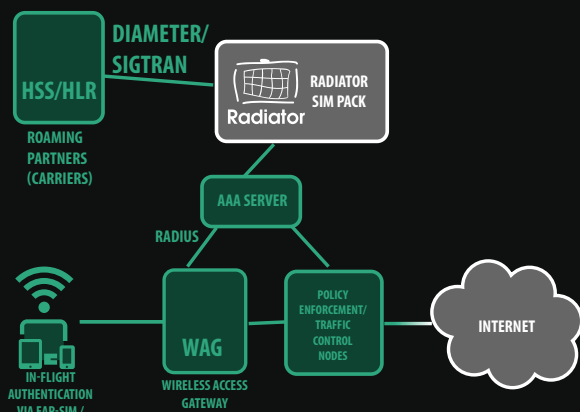
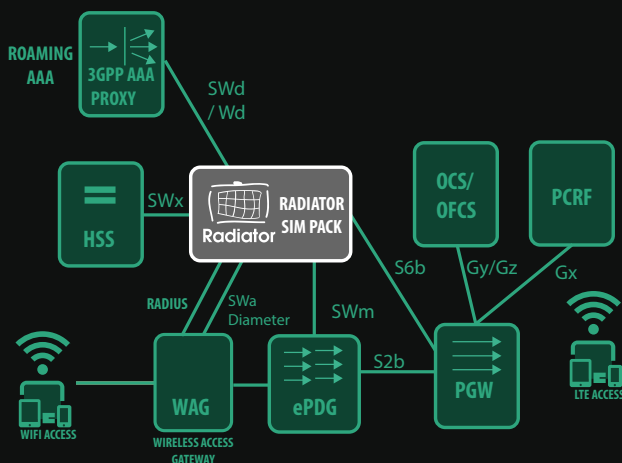
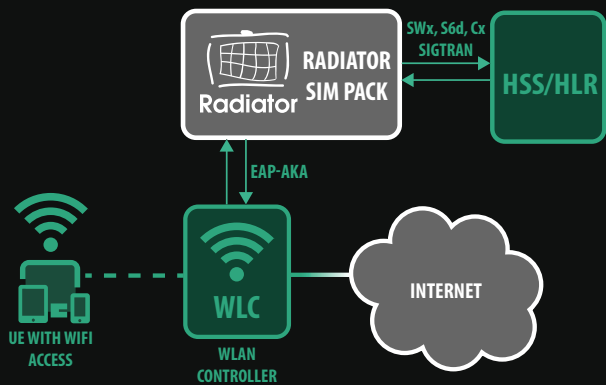
USE CASES FOR WI-FI SIM-BASED AUTHENTICATION

WI-FI OFFLOADING

In busy locations with high volumes of mobile traffic like sports stadiums, shopping malls, public transport hubs and underground metros, SIM-based devices can automatically switch from mobile data connections to local Wi-Fi networks. Transferring the data traffic to Wi-Fi networks reduces the load on the mobile network, which improves the coverage and the user experience. This is called Wi-Fi offloading.

WI-FI ROAMING

When a SIM-based device automatically joins a Wi-Fi network or switches to another one, this is called Wi-Fi roaming. Wi-Fi roaming is used to maintain an uninterrupted data connection when the user moves from location to location, or when the current Wi-Fi connection is overloaded or when the signal is weak.



VOICE OVER WI-FI

SIM-based devices can also switch LTE voice calls from mobile networks to Wi-Fi networks, and this kind of call is known as Voice over Wi-Fi. As with data traffic, switching traffic from regular calls onto Wi-Fi networks can help carriers and operators to reduce the load on the mobile network, enabling better call quality and continuity.

INDOOR, INFIGHT AND UNDERGROUND WI-FI NETWORKS

In locations such as underground metro stations and on commercial flights where mobile data signals are unavailable, SIM-based devices can switch automatically to local Wi-Fi networks provided in partnership with mobile carriers.

SECURITY ISSUES WITH SIM-BASED AUTHENTICATION IN WI-FI NETWORKS

When a SIM-based mobile device attempts to join a new Wi-Fi network, the network will request the user's identity – the IMSI – as authentication. However, with EAP authentication requests, this will be sent unprotected. This means that malicious actors can use Wi-Fi sniffers to see the identity of the user and their device.

PRIVACY RISKS WITH SIM-BASED EAP METHODS

Sending an unprotected IMSI creates significant privacy and security risks for the user. For example, in Evil Twin

or Honeypot access point attacks, a malicious actor can attempt to steal the users' identity, as well as tricking them into attempting authentication with an insecure Wi-Fi access point. This reveals the user's location and identity, making their device, communications and data connections more vulnerable to hacking and theft.

If a Wi-Fi network does not use IMSI Privacy Protection then the user's identity will be sent unprotected.

DRIVERS FOR SECURE WI-FI SIM-BASED AUTHENTICATION

PRESSURE FROM MOBILE OS MANUFACTURERS

The latest SIM-based Android and iOS devices already require secure IMSI authentication by default, and they will give a security alert and may refuse to join networks which do not have it in place. Without this secure authentication, it is possible that Wi-Fi roaming will fail for all modern SIM-based mobile devices.

THE WI-FI OFFLOADING AND WI-FI ROAMING MARKET IS GROWING

Wi-Fi offloading and roaming services are growing in popularity. However, there is also an increasing awareness of cybersecurity among businesses and consumers, as well as a growing number of threats. In particular, Wi-Fi sniffers have been recognised as a threat on Wi-Fi networks. Therefore, companies that provide Wi-Fi offloading and Wi-Fi roaming services need to improve the security of device authentication as they grow their businesses and expand their coverage.

WI-FI OFFLOADING IMPROVES PROFITABILITY

Wi-Fi offloading can bring several cost benefits to carriers and operators. For example, Wi-Fi connections are cheaper to provide than mobile connections, so Wi-Fi offloading enables carriers to relieve both load and cost on congested mobile networks. However, when Wi-Fi offloading works properly, switching connections should be seamless and invisible. Without a standard and secure method of Wi-Fi SIM-based authentication, this is not possible.

THE NEED TO IMPROVE THE USER EXPERIENCE

On Wi-Fi networks without secure IMSI authentication, users will get a privacy warning on their device if it tries to connect to an insecure network. Depending on the device, operating system and carrier settings, they may still be able to join the network or the device may refuse to connect entirely. Either way, the user experience is bad and secure Wi-Fi SIM-based authentication would improve it.



THE SOLUTION IS IMSI PRIVACY PROTECTION FOR WI-FI

To overcome the existing shortcomings and security risks in Wi-Fi SIM-based authentication, the Wireless Broadband Alliance (WBA) has developed the IMSI Privacy Protection for Wi-Fi standard. This standard specifies how to ensure enhanced privacy for SIM-based devices.

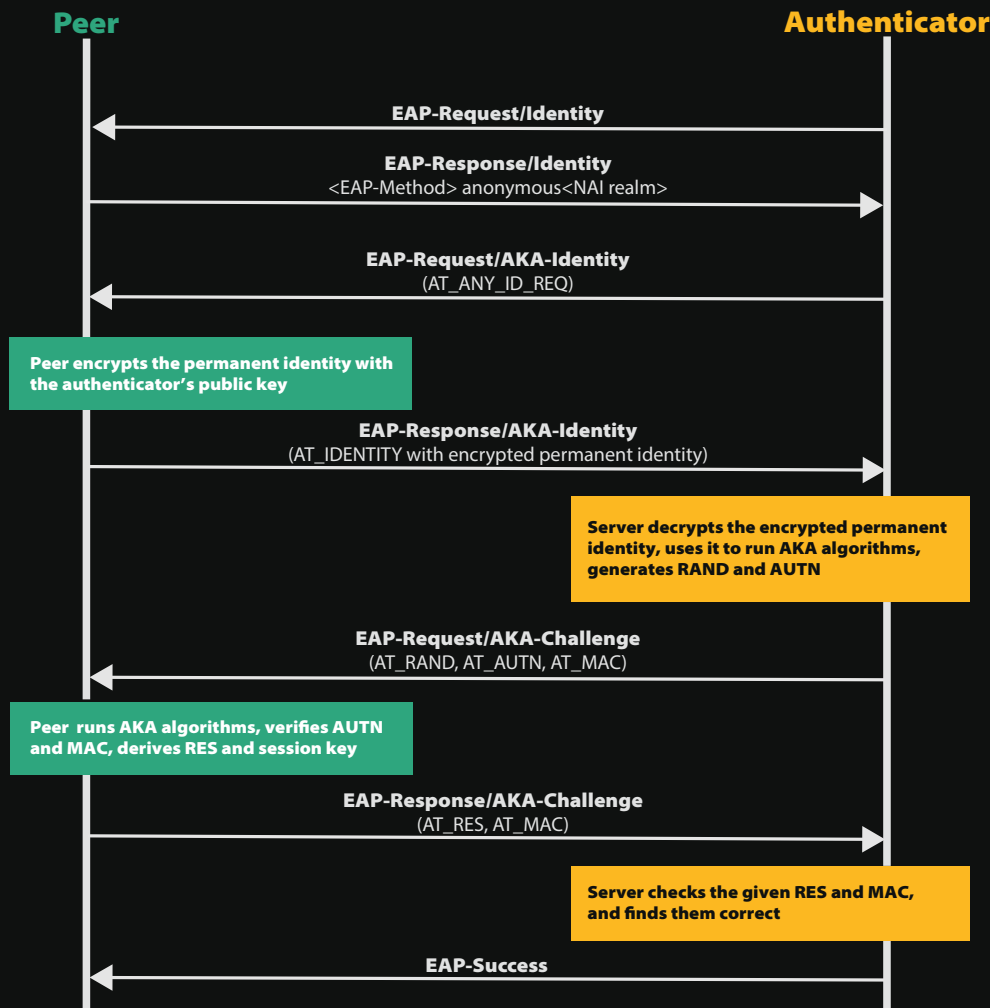
HOW DOES IMSI PRIVACY PROTECTION FOR WI-FI WORK?

When a SIM-based mobile device tries to join a Wi-Fi network with IMSI Privacy Protection enabled, the user's IMSI identity is encrypted on the device prior to being sent. Authenticator then grants the user's device

a temporary identity – also encrypted – so that the peer needs to send the IMSI only once. This keeps the user's identity private whenever their device connects to that Wi-Fi network.

This means that even if a Wi-Fi sniffer intercepts the request to join the network, it cannot obtain the user's real identity, nor can it track the location or activity of the user when they rejoin the network at a later date.

Some mobile OSs will not allow a device to authenticate unless it has secure IMSI authentication in place.



WHO IS RESPONSIBLE FOR IMPLEMENTING IMSI

PRIVACY PROTECTION FOR WI-FI?

Although Wi-Fi infrastructure may be owned and operated by different types of organisations or businesses, like venues and facility owners, typically, mobile operators are responsible for implementing IMSI Privacy Protection. This is because mobile operators are the Identity Provider (IdP) – they provide the SIM cards required for authentication and therefore they are the only party that actually handles IMSI authentication.

Mobile operators decide upon the security requirements for their networks and customers, and they provide the settings needed to enable IMSI Privacy Protection for Wi-Fi for all supported devices on their network. Depending on the market, mobile manufacturers may also provide operator-specific packages with all the settings included, which the devices can download. These packages will include the specifications for supported networks and the necessary security certificates.

WHAT DO YOU NEED TO IMPLEMENT IMSI PRIVACY PROTECTION FOR WI-FI?

Operators need a software solution that supports their AAA servers with IMSI encryption as specified in the WBA's IMSI Privacy Protection for Wi-Fi – Technical Specification.

THE RADIATOR SIM PACK FROM RADIATOR SOFTWARE IS ONE OF THE FIRST SOLUTIONS THAT SUPPORTS THE SPECIFICATION.

CUSTOMER CASE

Radiator Tier 1 mobile operator customer in Asia uses Radiator SIM Pack with IMSI Privacy as a part of their WiFi offloading solution. As the customer operates both their mobile network and over 50,000 WiFi hotspots in the advanced market, they need to ensure that WiFi offloading is both reliable and secure. With IMSI Privacy feature in use, the end users seamlessly join the WiFi network without worrying about privacy issues or warnings coming from their iOS or Android devices.

The IMSI Privacy feature for the customer was developed together with the Radiator team and our local partner, and is now a standard feature in the Radiator SIM Pack product.

IMSI PRIVACY PROTECTION ENABLES A GOOD WI-FI ROAMING EXPERIENCE

With IMSI Privacy Protection, Wi-Fi SIM-based authentication is seamless and invisible to the user. Device authentication happens automatically, so the user does not need to enter a username or password, and their connection continues uninterrupted.

Link to specification:

WBA IMSI Privacy Protection for Wi-Fi – Technical Specification:

<https://wballiance.com/resource/imsi-privacy-protection-for-wi-fi/>

ABOUT THE RADIATOR SIM PACK

The Radiator SIM Pack for Radiator AAA Server Software makes it easy for operators to enable IMSI Privacy Protection. It is the key component needed for secure and seamless switching between mobile and Wi-Fi networks using SIM-based authentication. The Radiator SIM Pack also provides all the functions required for a 3GPP AAA Server.

IMSI privacy is a key feature of the Radiator SIM Pack, and it provides server-side support for permanent identity protection during Wi-Fi SIM-based authentication, Wi-Fi offloading and VoWiFi, resulting in a higher quality user experience.

IMSI PRIVACY IS A KEY FEATURE OF THE RADIATOR SIM PACK.

The Radiator 3GPP AAA Server can handle both encrypted and clear authentication requests, which lets operators offer IMSI Privacy Protection to devices that support it without affecting other users. Radiator Software also provides the full source code with the Radiator SIM Pack.

The Radiator SIM Pack's IMSI Privacy features have already been in use by operators since early 2020, and it has proven to be reliable and secure.

BENEFITS OF THE RADIATOR SIM PACK:

IT'S INTEROPERABLE

You can integrate the Radiator SIM Pack with your company's own setup, including billing, CRM and business support systems.

- Radiator Software's products are compatible with all common platforms
- Proven interoperability with different device manufacturers
- No network infrastructure vendor lock-in

Radiator Software's products have a proven track record of interoperability with different platforms.

SIM-based authentication support for Radiator AAA Server Software is available through the Radiator SIM Pack, which includes:

- Full 3GPP AAA Server functionality for VoWiFi, VoLTE and WiFi offloading
- Standalone support for all SIM-based (EAP-SIM, EAP-AKA, EAP-AKA') authentication protocols for Wi-Fi offloading

IT'S EASY TO IMPLEMENT FOR WI-FI NETWORK DEVICES

With the Radiator SIM Pack you can introduce IMSI Privacy Protection gradually while still serving all customer devices, even older models without IMSI support.

- Simply upgrade existing Wi-Fi networks, there's no need to build a new one
- No specific hardware required
- Implement IMSI Privacy Protection without affecting the user experience
- No need for users to change SIM cards because IMSI Privacy Protection is handled by the Radiator SIM Pack
- End users don't need to take any action at all

ABOUT RADIATOR SOFTWARE

Radiator Software is a Finnish company that develops the Radiator AAA Server Software. Radiator is the leading solution for authentication, authorisation, and accounting (AAA) which allows you to control access to your wired and wireless networks comprehensively and efficiently.

Hundreds of companies and organisations around the world use Radiator for their AAA needs. Radiator provides RADIUS, RadSec, Diameter, and TACACS+ AAA interfaces with backends ranging from simple files to a carrier-grade 3GPP Diameter infrastructure. Radiator was first released in 1998 and remains under active development. Radiator SIM Pack provides reliable and effective security for Wi-Fi SIM-based authentication.

RADIATOR SOFTWARE IS A MEMBER OF THE WBA

Wireless Broadband Alliance is the global organisation promoting the latest Wi-Fi initiatives and standardisation within the Wi-Fi industry. WBA's membership consists of major operators, identity providers and leading technology companies across the Wi-Fi ecosystem. Radiator Software has been a WBA member since 2020 and remains committed to implement the industry best practices - such as WBA's IMSI Privacy Protection for Wi-Fi Technical Specification - into Radiator products.




GET IN TOUCH


Contact us to find out more about the Radiator SIM Pack and how we can help you implement IMSI Privacy Protection for Wi-Fi for your customers.

CONTACT DETAILS

RADIATOR SOFTWARE

Varastokatu 3 A
33100 Tampere
Finland
+358 45 1266 895
sales@radiatorsoftware.com
www.radiatorsoftware.com

 @RadiatorAAA

 radiator-software