alepo | Solution Brief

WiFi Calling

Introduction

Offering WiFi services is one of the best ways for mobile network operators (MNOs) to protect their core business. WiFi calling, or Voice over WiFi (VoWiFi), presents an opportunity to introduce carrier-class WiFi services that innovate, expand network coverage, and provide alternatives to OTT players like Skype and WhatsApp. In addition, MNOs who offer Voice over LTE (VoLTE) can provide seamless handoff from cellular to WiFi calls.

WiFi calling is an IMS-based service that allows users to make and receive calls (and send text messages) over a WiFi network instead of a traditional mobile network. The user's phone – a VoWiFi-supported device – has WiFi calling settings that can be turned on or off, provided it is supported by the operator. MNOs don't need to have their own WiFi network infrastructure in place; WiFi calling can be deployed without a single access point or partnership with service providers, as it can use public hotspots or home WiFi.

Alepo, an expert in carrier-class WiFi, offers vendor-agnostic solutions to bring WiFi calling to the market, regardless of the existing network type or business model.

Alepo's WiFi Calling Solution

Solution Benefits

- End-to-end solution
- Enables carrier WiFi calling over both untrusted and trusted WiFi networks
- ePDG and TWAG agnostic
- Fully integrates with IMS core to facilitate seamless handover between VoWiFi and VoLTE networks
- Secure connectivity and authentication for subscribers to transparently roam between 3G, 4G, and carrier WiFi networks
- Supports all 3GPP and 3GPP2 networks
- Minimizes total cost of ownership by optimizing upfront equipment CAPEX and reducing ongoing OPEX
- Industry-leading scalability with unique software-based solution

Solution Components

Alepo offers a cost-effective, easy-to-use solution to deploy VoWiFi, which includes:

Alepo AAA

AAA infrastructure serves as an important service and policy control framework to control how subscribers access and consume IP data services. Alepo's AAA is built to optimize network performance with carrier-grade authentication, authorization, and accounting. Alepo's AAA is an industry-leading product built for wireline, WiFi, and 3GPP mobile networks alike.

In WiFi calling, the Alepo AAA performs the following functions:

SWx to HSS	S6b to PGW	SWm to ePDG	SWa	STa
• Authorizes the user equipment and transports network-based mobility parameters to establish connectivity to the EPC	• Mobility-related authentication and authorization; creates a seamless handover when a user's device moves from WiFi to a cellular network, ensuring the call does not drop	• AAA signaling, including the transport of mobility parameters, tunnel authentication, and authorization data, also used for seamless handoff between LTE and WiFi networks	• Enables support for untrusted, non-3GPP IP access with the Alepo AAA. Also transports access authentication, authorization, and charging-related information securely	• Connects trusted non-3GPP IP access with the Alepo AAA, and transports access authentication, authorization, mobility parameters, and charging-related information securely

ePDG

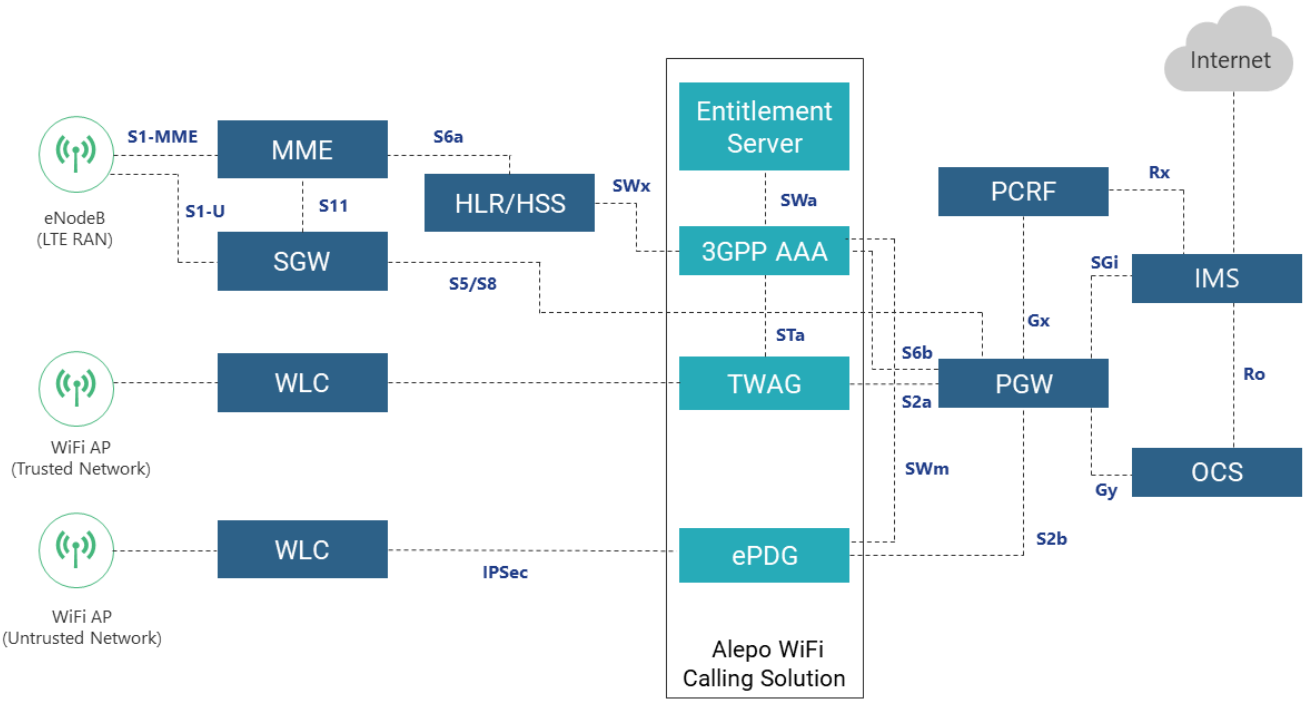
Non-3GPP access, like WiFi, can be split into two categories: "trusted" and "untrusted." Untrusted WiFi presents a challenge to mobile network operators. While trusted WiFi networks can interact directly with the EPC core, untrusted WiFi networks must interwork with the EPC core via a network entity called the ePDG (Evolved Packet Data Gateway). Security is achieved through the establishment of an IPSec tunnel between the user device and the ePDG. The tunnel protects both user equipment and the EPC core, allowing MNOs to securely deliver mobile packet core services over untrusted WiFi networks.

Entitlement Server

There are additional intricacies that operators face if they want to support rather than offer Apple devices, such as the iPhone, on their VoWiFi networks. Apple created a proprietary protocol, the Entitlement Layer Protocol, which is required for VoWiFi operation on any Apple device. This protocol validates the device for WiFi calling and aids in the collection of federally mandated emergency contact information (E911). However, each individual operator is responsible for implementing this. An Entitlement Server simplifies and speeds up the process of entitlement by bundling device enablement and E911 data collection into a consolidated solution that has a flexible deployment model and can be seamlessly integrated into an operator's existing mobile infrastructure. Alepo's AAA connects to the entitlement server over the SWa interface to connect the device to untrusted, non-3GPP IP access, and authenticate and authorize the user equipment for access to the evolved packet system.

TWAG

The key piece of network equipment that is required for trusted access is the Trusted Wireless Access Gateway (TWAG). The TWAG supports the interworking between the mobile packet core and trusted WiFi networks. It allows user equipment (phone, tablet, modem, etc.) to connect to the WiFi core. It is connected directly to the PGW in the mobile EPC through a secure tunnel (GTP, MIP, or PMIP). The TWAG interfaces with the AAA server via the STa interface to relay authentication credentials between the two. These credentials are then passed on to the HLR/HSS for final processing.



Through partnerships with ePDG, P-GW, TWAG, and entitlement server vendors, Alepo can offer an end-to-end, turnkey solution.

Deploying with Alepo

A Zero-Impact Solution

Making system-wide changes in a complex network environment can cause service disruption and require significant time and investment, delaying Time to Market (TTM). Alepo's WiFi calling solution allows rapid and cost-effective deployment by employing an existing WiFi infrastructure. With full support for EAP technology, this solution requires a minimal upgrade of network elements. In addition, Alepo's "replace nothing" deployment mode ensures seamless integration with existing network elements. By delivering only the necessary components to "bridge the gap", this approach reduces network complexity and unnecessary changes to the existing network environment, speeding up deployment time.

Any Hardware. Any Network Stack.

Alepo's solution simplifies integration and allows service providers to build a best-of-breed stack, not just now but also as the business evolves. The solution is field-tested and has been integrated with all major WiFi access network providers and is interoperable with various access networks.

Ongoing 24x7x365 Support

Alepo's Global Technical Assistance Center (GTAC) is an internationally renowned technical support services department, offering convenient, multi-channel, 24/7/365 support in a host of languages. The department operates in-house, ensuring quality checks at every level. The team comprises skilled, experienced support professionals and engineers, who provide immediate response, technical assistance, and implementation services to clients. All Alepo clients can subscribe to GTAC on an annual or multi-year basis.

A Best-Fit Solution

A modular and flexible architecture ensures components can be configured in any number of ways to find the best match for each customer. A custom solution is then constructed according to Alepo's core design principles of listening to our customers, automation, compliance to standards, scalability, feature-richness, flexibility, and future-readiness. The solution is measured against a rigorous set of key performance indicators (KPIs). On every project, Alepo carefully designs, builds, and delivers solutions that:

- Grow with the business and readily adapt to market changes
- Heighten the user experience for end customers and system users alike
- Reduce time, costs, and risks associated with deployment and network integration
- Maximize return on investment (ROI)

WiFi Calling Use Case Examples

WiFi Calling on Operator's Own Trusted Hotspot Network

Mobile operators can implement their own WiFi network in high-traffic or low-signal areas throughout the city and allow their customers free access, offloading them automatically if the cellular signal is congested or low.

WiFi Calling on Trusted Partner Public WiFi Network

Mobile operators can form partnerships with other WiFi networks, utilizing their pre-existing networks to increase their coverage area without any investment in infrastructure. The end user experience is just as seamless and automatic as it would be if they were using their own WiFi network.

WiFi Calling on Untrusted Public WiFi Network

WiFi calling works on any WiFi network. If the user has login credentials for the WiFi, they will be automatically connected to the network. The end user experience is just as seamless and automatic as it would be if they were using their own WiFi network.

WiFi Calling on Trusted Partner ISP WiFi Network

Mobile operators can form partnerships with ISPs or MNOs who have WiFi networks. These partnerships can be local or international, helping increase coverage without any investment in infrastructure. The end user experience is just as seamless and automatic as it would be if they were using their own WiFi network. The ISPs and MNOs who provide the WiFi can form agreements, charging the MNO for data their users consumed while roaming on the local WiFi network. The MNO can choose to pass this cost to the end user or provide international WiFi roaming as a free value-added service.