# Contents

1. Why consider VoWiFi?  
2. User experience requirements  
3. Mobile operator vs. OTT services  
4. VoWiFi client options  
   4.1 Integrated VoWiFi client  
   4.2 Separate VoWiFi client  
   4.3 Browser VoWiFi client  
5. Key Wi-Fi access characteristics to consider  
6. Technology options for VoWiFi services  
   6.1 VoWiFi using Evolved Packet Core  
   6.2 Direct access to VoWiFi  
   6.3 Mobility scenarios with VoWiFi  
7. Implementing security in VoWiFi  
8. Maintaining Quality of Service  
   8.1 Prioritizing traffic in IP networks  
   8.2 Prioritizing traffic in the operator’s core network  
   8.3 Quality of Service in Wi-Fi radio access  
9. VoWiFi performance considerations  
10. VoWiFi solutions from Nokia Networks
1 Why consider VoWiFi?

Many mobile subscribers will first look for a nearby Wi-Fi service rather than using their cellular network subscription for data services on their smartphones, tablets and laptops. Such behavior is helping to ensure that Wi-Fi remains the dominant way to access data services from smartphones and tablets:\(^1\)

- Smartphone and tablet users globally passed the landmark of 10GB of data consumption per user in December 2014. This includes Wi-Fi and cellular and is up 51% from 6.9GB per user in January 2014.
- Wi-Fi accounted for 80% of data consumption on smartphones and tablets, with cellular access playing a vital, yet supporting role.

With people being so accustomed to using Wi-Fi, many mobile operators can see significant business potential in offering Voice over Wi-Fi (VoWiFi) in homes and enterprises, extending the coverage they provide with LTE and 2G/3G networks.

To date, VoWiFi has been available to mobile users almost solely on over-the-top (OTT) smartphone and tablet clients from different vendors. Now as Voice over LTE (VoLTE) becomes more widely established, device makers are increasingly implementing a complementary VoIP client for Wi-Fi in the terminal chipset.

This integrated client makes the introduction of VoLTE and VoWiFi transparent to users because making a voice call is the same for both services, just press the green button.

VoWiFi helps to solve the challenge of indoor access for mobile users and can also reduce or eliminate roaming costs because calls may be treated as being local. Many mobile operators also see value in offering Wi-Fi services as a differentiator from over-the-top (OTT) providers.

The document **IMS over Wi-Fi** (GSMA IR.51) based on the **IMS Profile for Voice and SMS** (GSMA IR.92) and **IMS Profile for Conversational Video Service** (GSMA IR.94) identifies a minimum, mandatory set of features that are defined in 3GPP specifications. A wireless device and network are required to implement these features to guarantee interoperable, high-quality, IP Multimedia Subsystem (IMS)-based telephony and conversational video services over Wi-Fi access networks.

VoWiFi complements VoLTE because both are IMS-based services that can offer mobility and added-value services such as video and Rich Communication Services (RCS). Using the same IMS core infrastructure, a VoWiFi service can be launched before, after or at the same time as VoLTE.

A single architecture and infrastructure ensures that VoWiFi call routing, service subscription, billing and service execution are equivalent to VoLTE.

---

\(^1\) Smartphone and tablet usage trends and insights 4G LTE and Wi-Fi power and data consumption, Ovum 2015
giving a unified and secure identity for each user and major cost savings for the operator. (Table 1)

This white paper describes the key factors that operators will need to consider in planning and deploying a VoWiFi service, including device clients, security, Quality of Service (QoS), performance and network technology options. To address the uncertainty around Wi-Fi QoS, the paper also recommends using the cellular network for mobile voice whenever possible, with Wi-Fi supporting calls when cellular is not available.

2 User experience requirements

An important success factor is a simple, common user interface for both cellular and VoWiFi calls, with user preferences that are easy to activate and deactivate. The voice service must also allow the same mobile number and phonebook to be used for outgoing and incoming calls and messages, whether they are carried on the cellular network or as VoWiFi.

User devices should indicate whether the Wi-Fi or LTE network is in use, although when receiving a call, the user does not need to know whether it is coming in over Wi-Fi or LTE. It is vital to ensure seamless connectivity to a Wi-Fi access point and to smoothly continue a call from one access type to another. Communication confidentiality and security are essential, while speech quality and service availability should be at least as good as in other mobile voice services. Billing for the VoWiFi service should be easy to understand.

Although an operator has less control of VoWiFi speech quality and service availability when the service is accessed via a generic, third party Internet hotspot, users can accept these variations if the service provides additional value such as extended coverage or lower cost. Typically, a device using VoWiFi has a connection manager that measures the service experience received from network, and is capable of deciding which access is best to use. An operator’s customer service staff will need to be able to troubleshoot VoWiFi issues efficiently in order to help improve the call experience.

Table 1: The benefits of a single IMS architecture for VoLTE and VoWiFi services

<table>
<thead>
<tr>
<th>Easy</th>
<th>One number, service parity across access methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access</td>
<td>Works across LTE, Wi-Fi and fixed access</td>
</tr>
<tr>
<td>Built-in</td>
<td>One user interface, any device</td>
</tr>
<tr>
<td>Mobile</td>
<td>Service continuity across networks</td>
</tr>
<tr>
<td>Secure</td>
<td>Confidentiality and fraud protection</td>
</tr>
<tr>
<td>Services</td>
<td>Fulfill regulatory requirements and extend innovations</td>
</tr>
</tbody>
</table>

networks.nokia.com
3 Mobile operator vs. OTT services

Mobile operator and OTT provider VoWiFi services are distinctly different. Operator-provided VoWiFi is an extension of existing mobile communication services, while an OTT voice service is independent, although with similar characteristics. VoWiFi extends a mobile operator’s radio coverage and is typically paid for directly or bundled into a user’s existing mobile plan. OTT services are usually free, although the user may be billed for data usage and for breaking out of the OTT domain.

A user’s identity and typical mobile services are also available for VoWiFi, run by the same core network elements used for LTE access. In contrast, OTTs deliver services through their own servers and require a separate user identity.

Both operator VoWiFi and OTT services are offered over existing Internet access and carried over the Internet backbone, where guaranteed QoS is usually not available.

Table 2 shows additional factors in an operator-provided VoWiFi service on IMS architecture compared with the voice service offered by OTT providers.

Table 2: Operator-provided VoWiFi with IMS architecture compared with the voice service offered by OTT providers

<table>
<thead>
<tr>
<th>Services</th>
<th>Operator VoWiFi</th>
<th>OTT voice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile phone number</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Global phone number</td>
<td>Yes</td>
<td>Optional</td>
</tr>
<tr>
<td>Caller ID</td>
<td>Yes</td>
<td>Optional (separate new identity, never unified with operator-controlled identity)</td>
</tr>
<tr>
<td>Calls to/from PSTN</td>
<td>Yes</td>
<td>Optional (separate charges)</td>
</tr>
<tr>
<td>Service parity with 2G/3G</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IP messaging</td>
<td>Yes (Optional)</td>
<td>Yes</td>
</tr>
<tr>
<td>SMS messaging</td>
<td>Yes</td>
<td>Optional (separate charges)</td>
</tr>
<tr>
<td>Video calls</td>
<td>Yes</td>
<td>Optional (proprietary)</td>
</tr>
<tr>
<td>RCS services</td>
<td>Yes (Optional)</td>
<td>Yes</td>
</tr>
<tr>
<td>Regulatory requirements</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(eCall, Number Portability)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4 VoWiFi client options

Any VoWiFi service needs a voice client, which is an application that acts between the device’s user interface and its connection to external networks. The client also helps with user authentication when a call is placed over an untrusted Wi-Fi connection.

A client can be browser-based or a separate, downloadable application. Many new devices also include an integrated VoWiFi client. (Figure 1)

4.1 Integrated VoWiFi client

A VoWiFi client integrated in a device provides a seamless user experience for voice calls with either Evolved Packet Core (EPC) or direct-access IMS architecture. The user does not need to install additional software or perform any configuration tasks.

The user experience is better because short messages are stored in the device’s native messaging inbox and call history is stored in a unified call log, regardless of the access technology. There are also benefits in battery life and QoS implementations because these features usually reside in the device’s operating system.

For the operator, calls are managed in the same way as normal circuit-switched (CS) and VoLTE calls.

Close integration of the VoWiFi client offers additional benefits such as Subscriber Identity Module (SIM) authentication and seamless call continuity when the device moves outside wireless LAN (WLAN) coverage.

4.2 Separate VoWiFi client

A separate VoWiFi client application that is downloaded and installed by the user often leads to unfamiliar voice call features and service differences. However, a separate client may support services such as video telephony and Rich
Communication Suite. The client developer may also offer a device management server that is able to configure the VoIP application to meet operator preferences. Other drawbacks of using a separate VoWiFi client include:

- Different authentication methods
- Lower performance and inadequate user experience because the client is not optimized and its speech and video codec may not be supported by the cellular infrastructure
- Limited or no call handoff between different radios

Downloadable Wi-Fi clients fit with the Direct Access type of VoWiFi architecture.

4.3 Browser VoWiFi client

A web browser client is typically designed for laptops and tablets. Commercial web browsers such as Google Chrome, Mozilla Firefox and Opera support VoIP capabilities from WebRTC (www.webrtc.org). Being non-mobile, this approach is clearly different to any co-existing device-integrated client. Initial deployments may propose peer-to-peer approaches, while extension with IMS enables the use of public identity and interoperability with other networks and client types.

In core network web browser clients expect IMS to be extended with proper gateway functionality, typically co-hosted with IMS border control.

5 Key Wi-Fi access characteristics to consider

Voice calls need to be easy to use and delivered with very high quality and security. To meet these requirements, mobile operators can use the cellular network, with traditional or VoLTE technology, to handle voice traffic and offload the user’s data traffic to an available Wi-Fi network, especially if that network is untrusted for voice calls. For a roaming subscriber, VoWiFi needs to be optional and easy to use in order to avoid high roaming charges for phone calls.

Another challenge is obtaining the location information required by regulators for emergency calls made on a cell phone. In cellular macro networks, location information is standardized and available for all emergency calls. However, for Wi-Fi access, the location might be just an access indication and Wi-Fi access point MAC address, not its location.

For emergency calls, the subscriber’s phone needs to use either cellular macro access (2G/3G/4G) or the device needs to implement an option such as adding the latest macro access location. Additionally, operators might ask subscribers to provide VoWiFi location as part of their standard account information, such as when the service is used only in the subscriber’s home.

Making VoWiFi a 3GPP-standardized service will mean that users are securely authenticated, authorized and billed for usage. Standardization will also allow VoWiFi to work with any operator-provided fixed or mobile network and help produce a large ecosystem for the service.
This section outlines the key access characteristics an operator needs to consider when launching a VoWiFi service.

5.1 Ease of use

A voice call over an approved Wi-Fi network must be as easy to use as a voice call over a 2G/3G or LTE network, which means fully automatic connection to services. If the operator bundles Wi-Fi calling as part of a mobile subscription, user authentication should also be automated, possibly with the WPA2-Enterprise method.

When an operator sells Wi-Fi access as a separate service, for example at airports, the user may need to enter a username and password for access to an established account or a credit card number for access as a new user.

5.2 Security

Regardless of the client and core network used, the architecture must implement adequate security by authenticating the user either by SIM or other trusted credentials.

Additionally, proper encryption is required because unencrypted media streams can be easily intercepted from the Internet or unsecured IP backbone. The core network should also be protected from denial of service and other attacks.

When the VoWiFi architecture between the user device and the operator network is untrusted, the service access is based on EPC. The device and evolved Packet Data Gateway (ePDG) secure all communication using IPSec, which offers the same level of data integrity and protection as LTE using SIM credentials. This security design means that a voice service can be delivered over any Wi-Fi network.

With a Trusted architecture and EPC-based access, the use of WPA2-Enterprise authentication is mandatory. As well as radio and authentication security, operators also need to secure the transport link between the Wi-Fi access point (AP) and the Trusted Wireless Access Gateway (TWAG).

In the case of direct access to the operator’s network, security should be provided using IMS border control for the device, typically with Transparent LAN Service (TLS) for signaling and Secure RTP (SRTP) for the user plane. IPSec can also be used.

5.3 Quality of Service

Today, all Wi-Fi capable devices select a Wi-Fi network in preference to a 2G/3G or LTE data network. In a subscriber’s home, this automatic choice is usually trouble-free. However, for congested Wi-Fi networks (e.g., in a coffee shop), operators will want to use the cellular network for voice calls and Wi-Fi for data offload to avoid QoS issues. The device client makes the final decision to use a particular access based on internal measurements of the capability of the access to serve a real time service such as a voice call.
Poor Wi-Fi network and transport planning can result in inadequate capacity and poor voice call quality. Wi-Fi does not offer a QoS framework that is similar to 3G and LTE. Although a device and Wi-Fi AP can negotiate traffic characteristics and request resource reservation, these features are not universally supported by all manufacturers. Instead, the Wi-Fi Alliance (WFA) certified standard base Wi-Fi Multimedia (WMM) can prioritize video and voice in a Wi-Fi network.

6 Technology options for VoWiFi services

VoWiFi services with access network architectures are most efficient when using the unified IMS core network architecture. IMS can also support VoLTE and IMS Centralized Services (ICS) to unify services, billing and subscription data, as well as different kinds of access and devices.

The IMS architecture is the preferred way to deliver voice and multimedia services over IP networks. A common IMS core architecture provides voice services regardless of the access (Wi-Fi, LTE, CS) used, ensuring a consistent user experience with seamless handover and mobility between access methods.

Deployment of a VoWiFi service with an IMS core can be achieved with either of the following architecture options:

1. EPC with two sub-options, called “Trusted” and “Untrusted”
2. Direct access to IMS via an access border control system

These options meet the operator’s business requirements for specific features including voice and video telephony, messaging, user call management, location-based services and regulatory services. These VoWiFi deployment options also address issues such as the existing network architecture, mobility, security and device-side implementations.

Figure 2: Carrier IMS voice architecture options for VoWiFi
6.1 VoWiFi using Evolved Packet Core

IMS-based VoWiFi services can be accessed via the EPC using either Trusted or Untrusted access defined by 3GPP. Whether an access network is considered as “Trusted” or “Untrusted” is decided by the home network based on security features and other factors such as a business relationship.

In Trusted access, the Wi-Fi access points are connected to a Trusted WLAN Access Gateway (TWAG) network function that connects to EPC services via a standard interface. The device is required to support standard Extensible Authentication Protocol (EAP-AKA) authentication.

In Untrusted access, a device establishes a dedicated IPSec tunnel to an evolved Packet Data Gateway (ePDG) element located at the edge of the EPC. This IPSec tunnel transfers both signaling and media related to the operator services. The device is authenticated with EAP-AKA, which is mandated by 3GPP.

Untrusted access to EPC for VoWiFi enables mobility between Wi-Fi and LTE access networks whether or not a call is in progress. This mobility is performed at the EPC level, preserving the IP address allocated for the device. Internet traffic would not be directed to the EPC in Untrusted Wi-Fi access.

The use of an IPSec tunnel between the mobile device and ePDG is independent of the underlying access and ownership of the Wi-Fi access network, making Untrusted access applicable for a wider range of deployments.

When either Untrusted or Trusted access are deployed with VoLTE, a harmonized IMS core network architecture enables the same user services for both access types, as well as voice continuity between Wi-Fi and LTE.

6.2 Direct access to VoWiFi

The Direct Access option deploys voice and SMS over a Wi-Fi service without EPC involvement. User devices connect to the IMS system directly via Internet access using security measures such as Transport Level Security (TLS) or Secure RTP (SRTP) or by using an IPSec tunnel to a security gateway. The access border control solution provides the security and access control necessary to deploy voice and SMS over Wi-Fi.

The Direct Access option does not provide mobility between LTE and Wi-Fi radio networks. A call that moves outside the coverage of a Wi-Fi access point is likely to be released, although network functionality is available to solve this issue.

6.3 Mobility scenarios with VoWiFi

Maintaining a call between different access options can be achieved at the EPC level and the Session Initiation Protocol (SIP) application level. In addition, EPC mobility scenarios enable subsequent call handoff to LTE and CS networks with enhanced Single Radio Voice Call Continuity (e)SRVCC.
Implementing security in VoWiFi

Compared to VoLTE and CS voice, VoWiFi involves higher security risks. For example, hackers can use Denial of Service (DoS) attacks with hostile SIP clients via the Internet. Normal VoIP clients may exhibit attack-type behavior when affected by bugs and interoperability issues. Additionally, unencrypted media streams can be easily intercepted from an unsecured IP backbone.

Given these threats, implementing the right security measures is vital for VoWiFi services. These measures include encryption for protecting device communications and user identity. In a 3GPP Trusted network, encryption is used between TWAG and WLAN access security, and WPA2 is used between the device and the WLAN access. In a 3GPP Untrusted network, IPsec encryption is used between the device and the ePDG.

In Direct Access architecture, there is no EPC or authentication. Instead, signaling can be secured by using IMS border control and media can be encrypted with IPSec.
8 Maintaining Quality of Service

Voice quality is guaranteed with 3GPP radio standards, but Wi-Fi access brings new challenges to voice quality:

- Wi-Fi operates on unlicensed radio bands, so other radio equipment may interfere or compete for radio resources.
- Wi-Fi access to the operator's voice core may be over Internet Service Provider (ISP) networks, which cannot be managed by the 3GPP network operator.
- Multiple users and applications may cause congestion when sharing the same Wi-Fi network.

Addressing these QoS challenges requires different approaches to prioritizing traffic in each part of the call path.

8.1 Prioritizing traffic in IP networks

In backbone access and operator core networks, voice packets can be prioritized using Diffserv Code Point (DSCP) marking by the VoWiFi client in the user device. However, network elements may not accept this marking and so will give voice traffic the same best-effort bandwidth as any other data. To reduce bad user experiences, the VoWiFi devices should assess Wi-Fi access and select the best available prioritization method.

8.2 Prioritizing traffic in the operator's core network

The dedicated bearer for voice and video traffic is established during VoWiFi call setup based on the session description and qualitative values received from the IMS. These procedures are the same for VoLTE access in order to perform seamless mapping for handover of calls between Wi-Fi and LTE.
Downlink traffic is marked to enable prioritization in the IP backbone and in the Wi-Fi AP if supported. Similar traffic marking may be used for uplink traffic, according to the operator's configuration.

Unlike Wi-Fi access, LTE resources are allocated to ensure proper QoS for specific traffic. For mobility between Wi-Fi and LTE accesses, both connect to the Packet Data Network Gateway (PGW), which allocates an IP address to the user that remains the same during mobility. The PGW also keeps active existing bearers and ensures they are properly established in the target access and released in the source access.

### 8.3 Quality of Service in Wi-Fi radio access

The QoS architecture in Wi-Fi access is based on packet prioritization, not on resource reservations as in VoLTE and 2G/3G networks. Packet prioritization aims to ensure better latency and packet loss ratio for improved quality of voice calls.

When the operator controls the Wi-Fi network in a public place or office environment, it can prioritize access for VoWiFi traffic. In the Wi-Fi air interface, the WMM classification can be used to prioritize voice traffic between the user device and the AP. WMM enables a VoWiFi device client to prioritize the voice traffic uplink and for the Wi-Fi AP to prioritize the downlink.

In an operator-managed Wi-Fi network, the Wi-Fi AP can also categorize traffic when the source address of the IP packets points to an operator's core network elements. The Wi-Fi network may also provide mechanisms to identify VoIP traffic patterns to prioritize the voice traffic.
9 VoWiFi performance considerations

Unlike LTE, Wi-Fi access does not have guaranteed radio resource handling for voice traffic. Yet VoWiFi is expected to achieve comparable performance when the benefits of an integrated VoIP client, best Wi-Fi practices and optimized core network functionality are combined.

Nokia testing and live network operation of VoWiFi reveals several considerations for VoWiFi performance. First, voice quality as measured by Mean Opinion Score (MOS) remains the same as long as the IP transport has acceptable QoS (i.e., bit error rate, jitter, latency), sufficient bandwidth and adequate radio conditions.

For power efficiency, Wi-Fi access improves device battery life compared to cellular access in cell-edge conditions. Additionally, the mobile device may have implemented the WMM power-save mechanism, which enables sleep mode during voice service at applicable intervals (e.g., 20 ms).

In conditions where coverage is weak, the call-drop rate is similar to VoLTE where there is a handover from LTE to 2G/3G.

In addition, VoWiFi-enabled devices have a mechanism to measure the conditions of the Wi-Fi connection to determine if it is adequate for the voice traffic. These are proprietary implementations developed for the device chipset or VoWiFi client. For operator-managed Wi-Fi networks, 3GPP defines a mechanism for devices and access points to measure the Wi-Fi conditions.
10 VoWiFi solutions from Nokia Networks

The Nokia Networks mobile broadband portfolio for Voice over Wi-Fi covers the IMS, packet and mobile voice core networks, as well as indoor and outdoor and small cell Wi-Fi access. This portfolio matches today’s needs for Untrusted and Direct Access VoWiFi deployments.

The Nokia Voice over Wi-Fi solution is built on the market-leading Nokia Voice over LTE solution. This foundation ensures that operators deploying either of these access technologies will benefit immediately from the quality, unique feature set and end-to-end perspective of Nokia Networks products and services. The Nokia Networks solution is compatible with devices from leading vendors.

Nokia Networks IMS products are used today in many networks to provide services such as Voice over LTE, rich communication services, fixed network services and others. Voice over Wi-Fi is a natural evolution of these services.