SOLUTION BRIEF

How, When and Wi-Fi:

Weaving Wi-Fi into Your Network Experience through Virtualization

THE WI-FI OPPORTUNITY

While 4G and LTE have captured much of the media attention, Wi-Fi has quietly become the wireless network of choice for many subscribers. Today, more than half of all mobile traffic (60%) is carried over Wi-Fi networks in homes, offices and public places from coffee shops to shopping malls. With the number of Wi-Fi hotspots expected to quadruple globally to 5.8 million over the next few years, analysts predict that soon as much as 80% of all mobile voice and data traffic will be Wi-Fi based.

After years of building out their networks, fixed and mobile service providers now recognize the strategic necessity of bringing Wi-Fi access into their network experience. Extending their network coverage through Wi-Fi access enables today's service providers to solve some of their most pressing challenges:

- It enables network providers to monetize Wi-Fi communications through value-added services (e.g. security, quality, persistent identity);
- It allows service providers to compete more effectively with over-the-top (OTT) providers such as Skype and WhatsApp;
- It gives mobile providers a cost-effective alternative to extending their wireless network coverage into "difficult" areas (e.g., in-building coverage);
- It provides an inexpensive backhaul solution to offload the growing amount of video and data traffic on the macrocellular network

THE WI-FI CHALLENGE: SEAMLESS INTEGRATION

The challenge for fixed and mobile service providers is to seamlessly integrate Wi-Fi voice and data communications into their networks and effectively monetize Wi-Fi access through value-added services that include better quality of experience and seamless session handoff between networks. There are four key areas in which service providers can provide value through network integration:

1. Security
2. Session continuity

3. Policy/quality enforcement
4. Services such as content filtering, web and video optimization
5. Access to operator content ie. video, music etc

To support this integration, the telecommunications industry has defined two network elements to serve as a secure gateway between a service provider's core network—an evolved packet core (EPC) in the case of mobile service providers—and both trusted and untrusted Wi-Fi networks. For access to trusted Wi-Fi networks such as those deployed by or in partnership with the service provider, the industry has defined the **Trusted WLAN Access Gateway/Proxy (TWAG/TWAP)** as this secure entry point. For access to untrusted Wi-Fi networks such as those operated independently or in connection with another service provider, the appropriate network element to secure Wi-Fi access would be the **evolved Packet Data Gateway (ePDG).**

Currently, service providers have two options for deploying these elements in their network: either as a standalone, hardware-based legacy device (the traditional approach) or as a virtualized, software-based solution. Network functions virtualization (NFV) is fast becoming the new standard for network evolution as service providers look to scale their networks quickly while reducing complexity and cost. To meet this new demand, many legacy network gateway vendors are now adapting their hardware-based solutions for virtualized environments. Yet these solutions rarely offer the same robust performance and economic benefits that natively developed NFV solutions present.

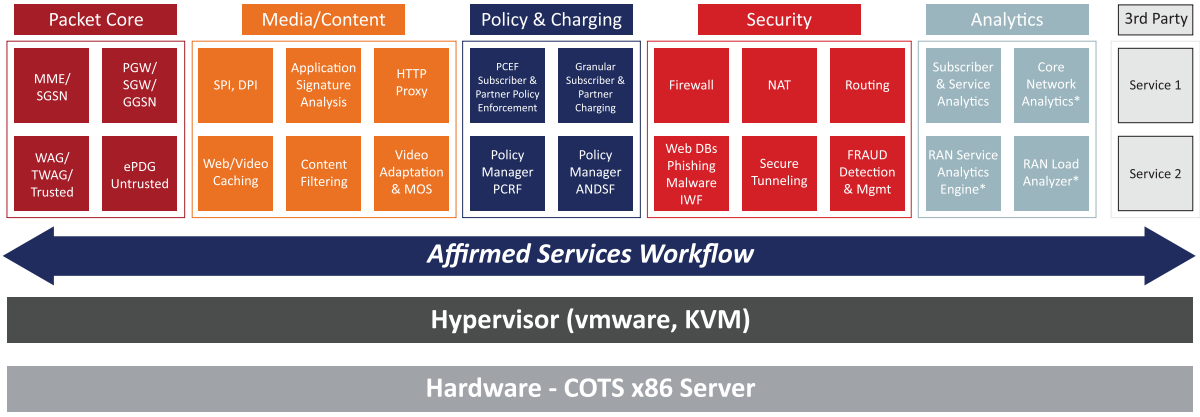

FIGURE 1: AFFIRMED MOBILE CONTENT CLOUD

THE AFFIRMED WI-FI GATEWAY SOLUTION

As a leader in the NFV network evolution, Affirmed Networks is helping fixed and mobile service providers build the next-generation of networks using carrier-class, natively virtualized solutions. Affirmed's groundbreaking virtual EPC (vEPC) solution, dubbed the Mobile Content Cloud (MCC), is currently deployed in some of the world's largest mobile service provider networks. The Affirmed Wi-Fi gateway has been developed on top of the MCC from which it inherits a wide range of mobile gateway functions such as GGSN, SAE-GW, SP/DPI/Heuristics application detection, PCEF with Gx and Gy interfaces for QoS and offline/online charging, Lawful Interception, as well as its rich set of content services such as HTTP(S) Proxy, web and video content optimization and adaptation, content caching, content filtering/parental control, subscriber firewall, NAT/ALG and more. The Affirmed Wi-Fi gateway solution features complete TWAG/TWAP and ePDG functions that can be deployed on commercial off-the-shelf (COTS) servers or within the vEPC on virtually managed hardware.

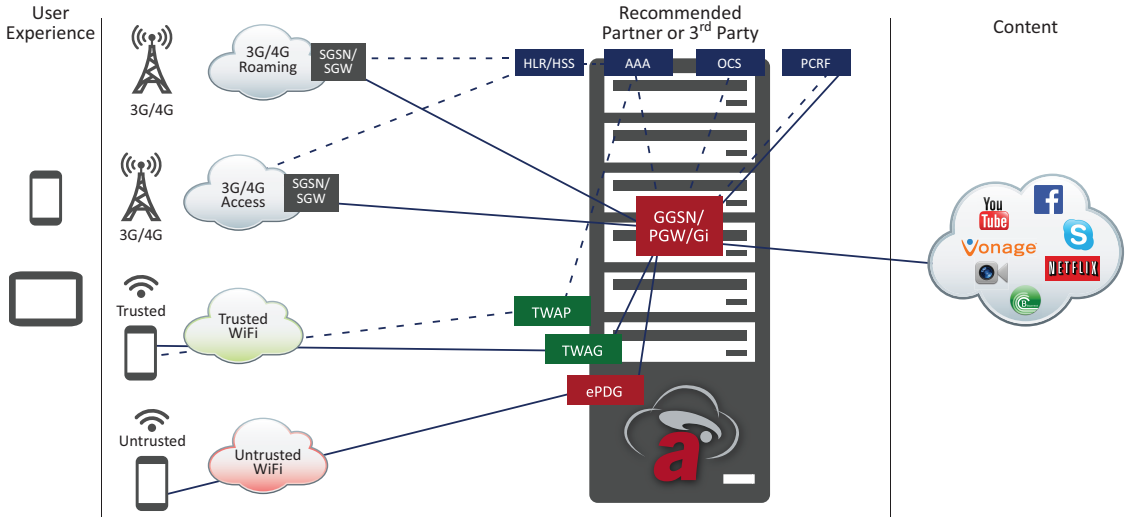

FIGURE 2: AFFIRMED WI-FI GATEWAY

Affirmed's Wi-Fi gateway solution is designed to provide the most robust, reliable and flexible solution on the market today, featuring:

- Ultra-high performance on commercial x86 servers and blades;
- Open support for popular hypervisors from VMware, KVM and OpenStack;
- Full compliance with ETSI NFV standards;
- Easy integration with the Affirmed vEPC or third-party EPC solutions;
- A uniquely engineered virtual ePDG that delivers 5G levels of performance for high volumes of encrypted traffic;
- Seamless delivery of core network services including policy/charging, packet inspection, value-added service/content optimization and workflow orchestration.

The Wi-Fi Gateway in Action: Four Examples

There are several ways that service providers can leverage Wi-Fi access to enhance their services and improve network performance. These include offloading traffic onto trusted Wi-Fi networks, extending core network services through trusted (and untrusted) Wi-Fi networks and providing VoWiFi or WiFi calling services which includes seamless session handoff between Wi-Fi and macrocellular networks. We'll take a look at each of these cases below and explain how the Affirmed Wi-Fi gateway solution the necessary integration to support these services.

Offloading Traffic onto Trusted Wi-Fi Networks

Using Wi-Fi networks to extend network coverage and reduce traffic on the macrocellular network has clear cost advantages for service providers. A trusted Wi-Fi network can be either a hotspot that the service provider maintains (e.g., a hosted hotspot at an airport) or one deployed in partnership with the provider. The service provider in this case may be a mobile or a fixed network operator. Cable provider Comcast, for example, currently offers both wireless voice and data services through thousands of wireless hotspots that it has deployed in the U.S.

By a *trusted* network, we mean one in which the service provider can verify basic user information and exert some level of control over the access point. In the example above, Wi-Fi users would be authenticated by the service provider's Authentication, Authorization and Accounting (AAA) system via the TWAP, while the voice/data traffic itself would pass through the TWAG an be offloaded onto the data network for backhaul. An added value that Affirmed's solution brings to this scenario is the ability to apply Gi services to the subscriber. These services include: Policy enforcement (including QoS policies), content filtering, web/video optimization and security services such as NAT, Firewall and IPS.

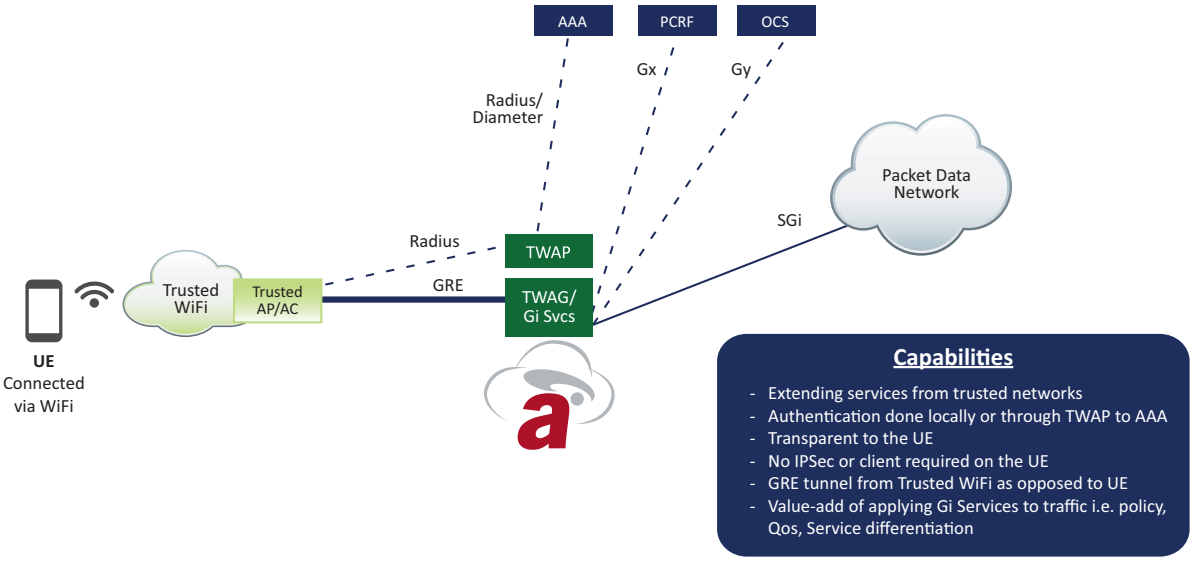

FIGURE 3: TRUSTED OFFLOAD

Trusted Wi-Fi Access Integration to EPC

Extending the subscriber's network experience—including value-added services and seamless session handoff—to trusted Wi-Fi networks requires tight integration with the service provider's core network. An example of trusted Wi-Fi access would be wireless roaming at a large shopping mall, where mobile subscribers would seamlessly move from the macrocellular network outside the mall to the wireless LAN (WLAN) once inside the mall. In such a scenario, subscribers would enjoy better wireless reception indoors without requiring them to log on to the network or interrupt existing sessions.

As in the example above, the TWAP would secure communications with the AAA server for authentication/authorization, while the TWAG would offload voice/data traffic (and enforce policies on that traffic) onto the packet data network. However, not all traffic may be routed directly to the Internet directly. Certain traffic may be routed through the TWAG to the packet core network. Operators would do this if they want to serve up hosted content such as video or music. The Affirmed TWAG supports the industry-standard S2a interface, which enables the TWAG to communicate directly with any industry-standard EPC gateway, whether it's part of Affirmed's virtual EPC solution or an existing third-party EPC solution.

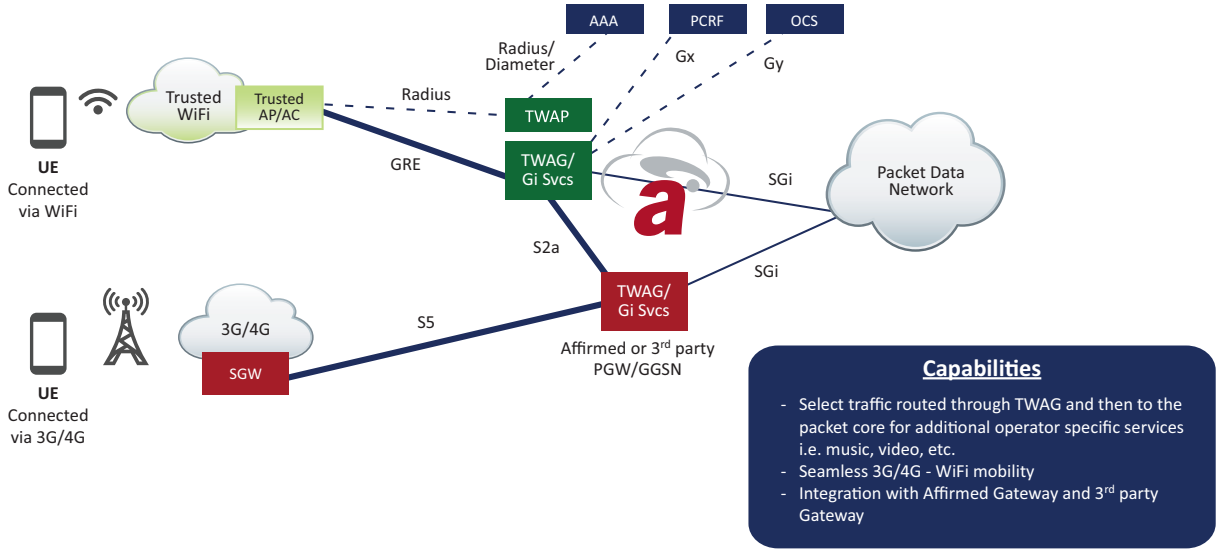

FIGURE 4: TRUSTED vEPC INTEGRATION

Untrusted Wi-Fi Access Integration

In a world with millions of Wi-Fi access points, untrusted Wi-Fi networks are a common occurrence. By an untrusted network, we mean one in which the service provider cannot authenticate users or control the flow of traffic over the network. An example of an untrusted network could be a Wi-Fi network in a coffee shop or one hosted by a competitive provider. In order to safely bring untrusted Wi-Fi networks into the core network, service providers must deploy a different element: an evolved Packet Data Gateway (ePDG).

Communications over untrusted networks require an added level of security known as IPsec encryption. Industry standards mandate that all mobile devices must feature an IPsec client on the device. In this case, voice and data sessions pass securely through an IPsec tunnel. These tunnels often need to remain open in anticipation of incoming or outgoing calls, so that at any given time millions of IPsec tunnels may need to remain open in the network. Hardware-based ePDGs are designed to handle this high demand for open IPsec tunnels, but these same high encryption requirements have historically proven problematic for virtualized ePDG instances. The Affirmed ePDG is the exception to that rule: a remarkably robust virtual ePDG that can deliver 5G levels of IPsec-encrypted communications on a single server.

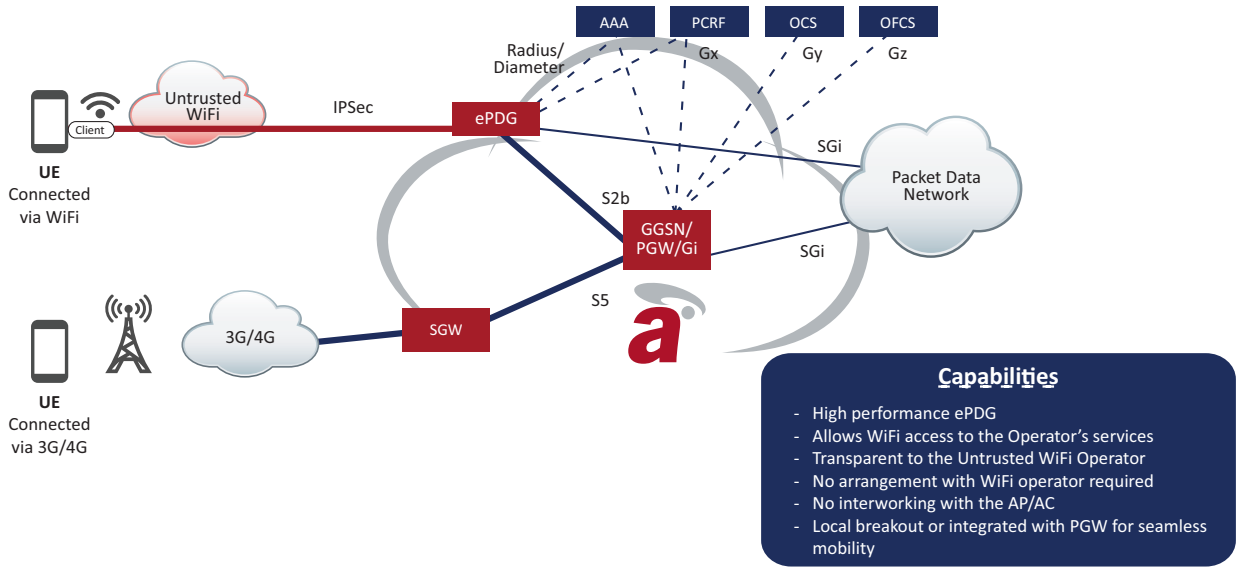

FIGURE 5: UNTRUSTED WI-FI vEPC INTEGRATION

Voice Over Wi-Fi

Much like Voice over LTE (VoLTE), Voice over Wi-Fi (VoWiFi) seeks to create seamless handoff between networks during a live voice call. Consider our earlier example of the shopping mall; in this case, service providers would be concerned with moving the session from the macrocellular network outside the mall to the Wi-Fi network inside the mall without dropping the session or requiring the user to log in to a different network. In fact, the goal with VoWiFi (as with VoLTE) is to make this transition completely invisible to users.

Although relatively new, VoWiFi is expected to gain traction in the coming years as mobile service providers look to address one of their greatest challenges: weak in-building coverage. The addition, for the first time, of built-in VoWiFi features into the new Apple iPhone 6 is expected to accelerate the adoption of VoWiFi.

The ePDG provides the necessary support for encrypted VoWiFi calls while bringing the session into the IMS/LTE core for persistent session control and policy enforcement. Here again, the Affirmed ePDG provides a superior level of performance on encrypted communications in a scalable, flexible virtualized platform.

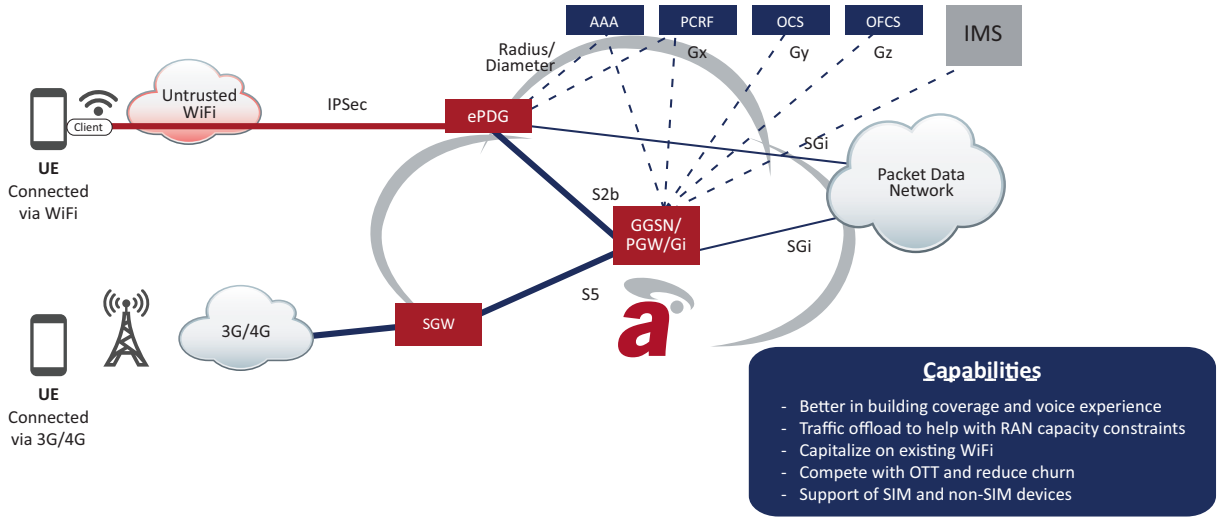

FIGURE 6: VOICE OVER WIFI

Making the Wi-Fi Future a Reality Today

Wi-Fi access is critically important to the future of fixed and mobile service providers—as important as radio access networks and potentially more important than VoLTE. Yet service providers need to solidify their Wi-Fi access strategies soon, as the key market players are already jockeying for position in this new market, as evidenced by early Wi-Fi service rollouts from T-Mobile and Comcast. Network functions virtualization provides the quickest and most cost-effective path for this transformation, provided that the solution delivers carrier-class security, seamless session handoff and tight integration with core subscribers services such as policy enforcement, identity and accounting.

Virtualization and Wi-Fi access present the next generation of networked communications. By bringing the two technologies together in a robust and highly scalable solution, Affirmed enables service providers to deliver a better communications experience for their subscribers through innovation and smarter efficiency.

APPENDIX

Wi-Fi Interfaces