EXPANDING THE SECURE DELIVERY OF ULTRA-BROADBAND MOBILE SERVICES OVER UNTRUSTED WI-FI

APPLICATION NOTE

Alcatel·Lucent

ABSTRACT

The Evolved Packet Data Gateway (ePDG) function allows operators to securely deliver mobile packet core services over untrusted, non-3GPP networks, including some Wi-Fi networks to any Wi-Fi-enabled device. This application note describes the ePDG function, how it addresses operators' key considerations for service delivery over untrusted, non-3GPP networks, as well as illustrating how the ePDG function is supported on the industry-leading Alcatel-Lucent 7750 Service Router Mobile Gateway (SR MG) platform.

TABLE OF CONTENTS

INTRODUCTION

The use of Wi-Fi-enabled devices is growing at an unprecedented rate. Juniper Research[1] suggests that, by 2017, mobile data traffic generated by smartphones, feature phones and tablets will exceed 90,000 petabytes, and that the majority of the data traffic (60 percent) will be via the Wi-Fi network. In some regions such as Europe, the percentages are even higher. The European Commission[2] reported that 71 percent of 2012 EU wireless traffic delivered to smartphones and tablets was over Wi-Fi and estimates that this will rise to 78 percent by 2016. Additionally, a report by Informa Telecoms and Media[3] indicates that "Wi-Fi hotspots are expected to grow from 1.3 to 5.8 million globally in the next four years."

In fact, Wi-Fi access has grown so quickly that, for mobile operators, the mushrooming of Wi-Fi-enabled devices and the "hop-on-any-Wi-Fi" option represents an enormous opportunity as well as a daunting challenge. Because Wi-Fi-enabled devices can access services without cellular service, operators must extend their service reach across the full range of Wi-Fi-enabled devices.

Historically mobile operators have tended to view Wi-Fi as an offload capability for Internet access. However, as they continue developing their data services portfolio, including voice, messaging, secure CRM-protected video delivery, and security (parental control and anti-malware etc.) all of which are delivered from their service LANs over their cellular radio access networks (RANs), they must look to extend the delivery of these services over other access networks, Wi-Fi included. For this to happen successfully, they need to provide the same secure authentication, confidentiality, billing and security as they do for their cellular RAN-delivered services.

To support this expanded service delivery footprint, the mobile industry and operators are embracing some 3GPP-defined options for service delivery over both trusted and untrusted non-3GPP access networks. These options include:

- Trusted Wireless Access Gateway (TWAG): The TWAG supports interworking between the mobile packet core and trusted Wi-Fi radio access networks (Wi-Fi RAN), which support capabilities that include 3GPP network access, secure authentication and RAN encryption.
- The Evolved Packet Data Gateway (ePDG): The ePDG gives operators the ability to deliver mobile packet core services over untrusted non-3GPP network access, which could include residential, public and enterprise Wi-Fi hotspots.

EXPAND THE POTENTIAL OF ULTRA-BROADBAND MOBILE SERVICES

Figure 1 illustrates how mobile operators are embracing the functionality offered by the 3GPP-defined Evolved Packet Data Gateway (ePDG) for the delivery of mobile packet services over untrusted non-3GPP access networks.

For its part, Alcatel-Lucent supports a full range of mobile gateway functions that are proven, robust, feature rich and reliable. These mobile gateways enable the delivery of ultra-broadband mobile services with exceptional performance and scale. They provide

[1] Juniper Research: Mobile Data Offload & Onload; Wi-Fi, Small Cell & Carrier Grade Strategies 2013-2017; April 2013.

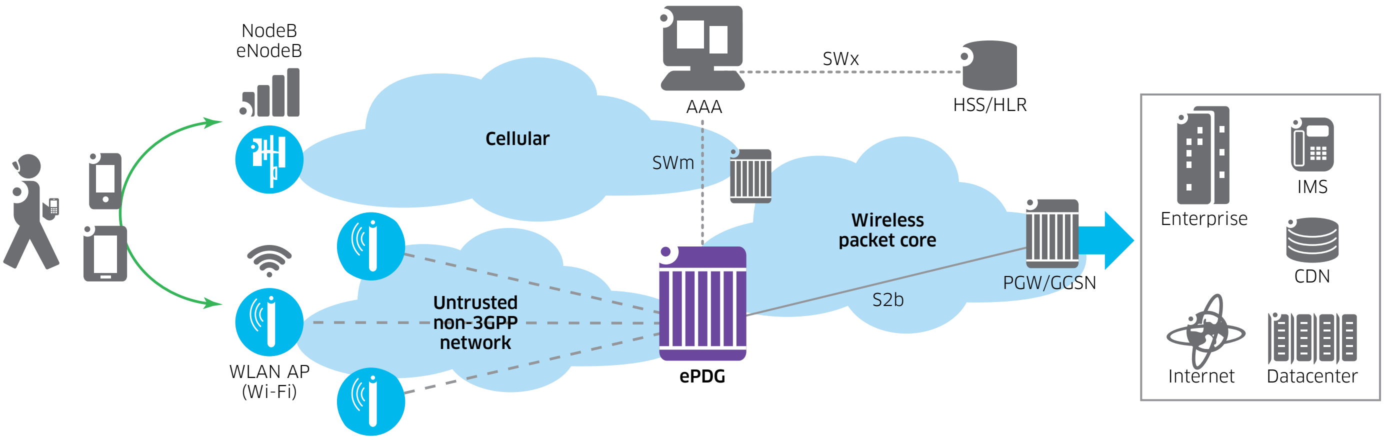
[2] European Commission: Study on Impact of Ttraffic Off-Loading and Related Technological Trends on the Demand for Wireless Broadband Spectrum; 2013

[3] Wireless Broadband Alliance (WBA), and compiled by Informa.

deployment flexibility and service agility with concurrent support for a wide range of mobile gateway functions, including:

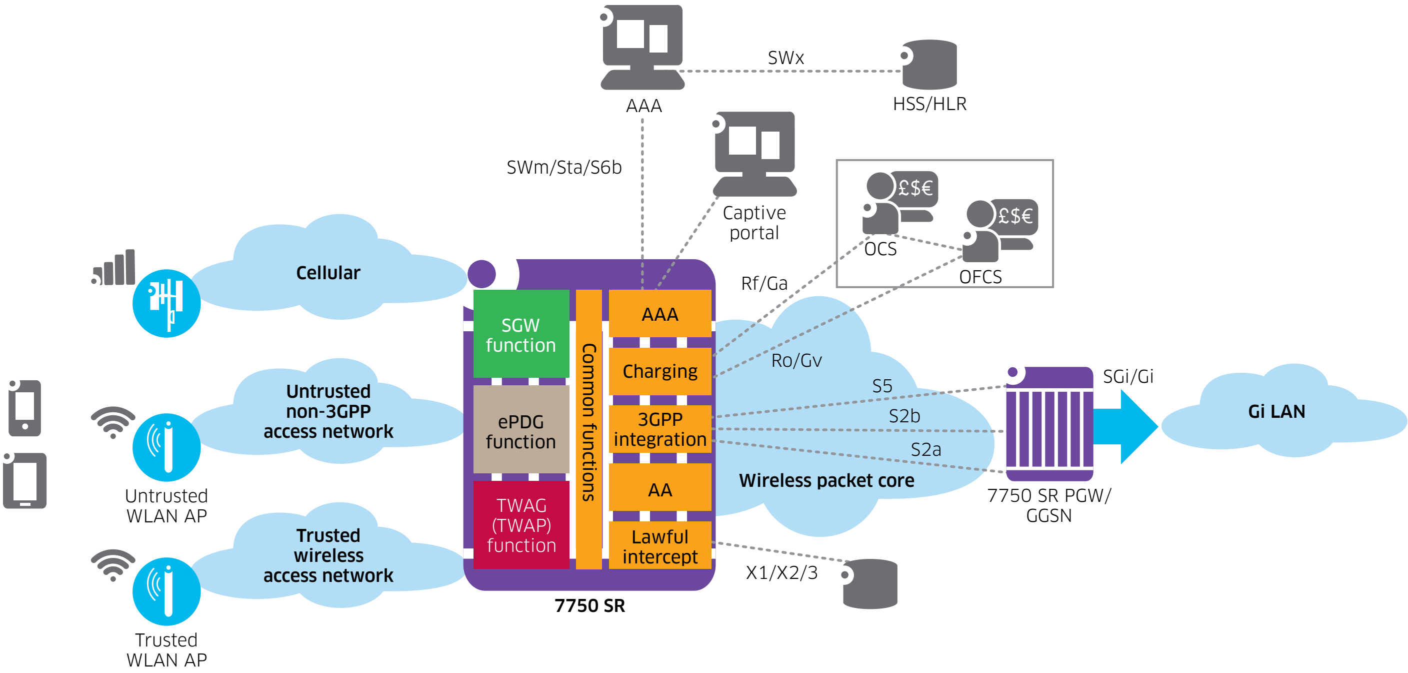
- Cellular gateways for cellular radio access networks (SGW/PGW/GGSN)
- Trusted wireless access gateways (TWAG) for 3GPP-trusted access networks
- Evolved packet data gateways (ePDG) for untrusted, non-3GPP networks

Figure 1. ePDG functionality delivers untrusted Wi-Fi access



All Alcatel-Lucent mobile gateway functions, including the ePDG, are supported on the industry-leading Alcatel-Lucent 7750 Service Router (SR) platform (see Figure 2). The 7750 SR architecture enables high-density service interfaces with low-power consumption per transported bit, while concurrently supporting processing-intensive gateway services with no trade-off between performance and advanced service delivery. The Alcatel-Lucent mobile gateway functions provide deployment flexibility and service agility with concurrent support for a range of mobile gateway functions on a single 7750 SR platform, including ePDG and PGW/GGSN.

Figure 2. Alcatel-Lucent 7750 SR Mobile Gateway: A single platform spanning all radio access technologies

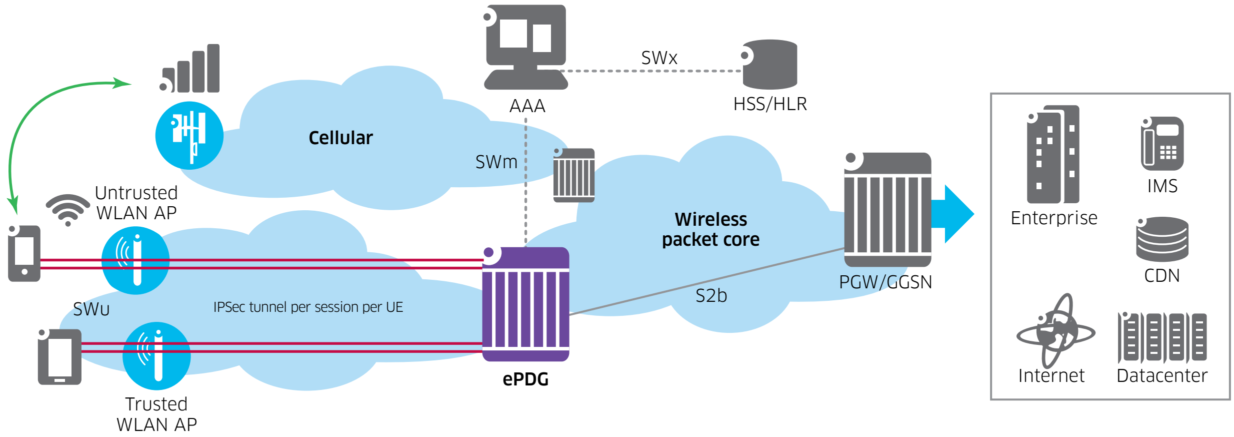


Because the mobile gateways span all radio access types, the ePDG can leverage the 7750 SR Mobile Gateway's common functions. These include the independent scaling of the control and user planes, Lawful Intercept, subscriber accounting and policy interfaces. Also supported is a range of IP networking capabilities such as L2 and L3 services, as well as IP/MPLS networking capabilities to support integration with existing networks. Each of these capabilities is critical for deployment support and flexible integration as mobile operators look to further extend their reach by delivering secure and reliable services, as well as applications over untrusted networks.

SECURE AND SCALABLE

As illustrated in Figure 3, the ePDG function supports secure access interworking between the mobile packet core and untrusted, non-3GPP networks. Security is achieved through the establishment of an IPSec tunnel between the user device and the ePDG. Once the local IP address is assigned to the device, the IPSec tunnel, which is transparent to the local Wi-Fi access point (AP), is established. The tunnel originates from the user equipment for each Packet Data Network (PDN) session, and protects both the user equipment and the wireless packet core.

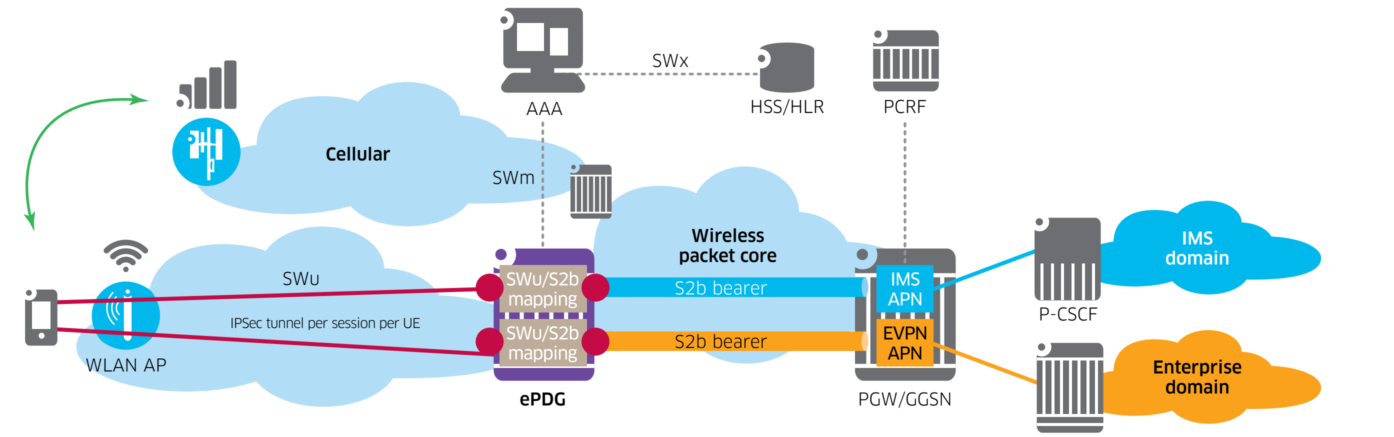
Figure 3. Untrusted Wi-Fi network architecture



MULTIPLE APN SUPPORT

With the addition of the ePDG function, the wireless packet core enables connections to different types of Access Point Networks (APNs) over a Wi-Fi connection. As shown in Figure 4, the multi-PDN/IPSec tunnel-capable user equipment initiates an IPSec tunnel for each Packet Data Network (PDN). This allows it to communicate with the correct downstream or service network. Next, the ePDG terminates the IPSec tunnel from the user equipment and directs the traffic onto individual S2b bearers. The S2b bearers are then terminated and transformed into specific instances on the Packet Data Network Gateway (PGW), allowing traffic to be directed to appropriate downstream or service networks.

Figure 4. Enabling multi-APN’s

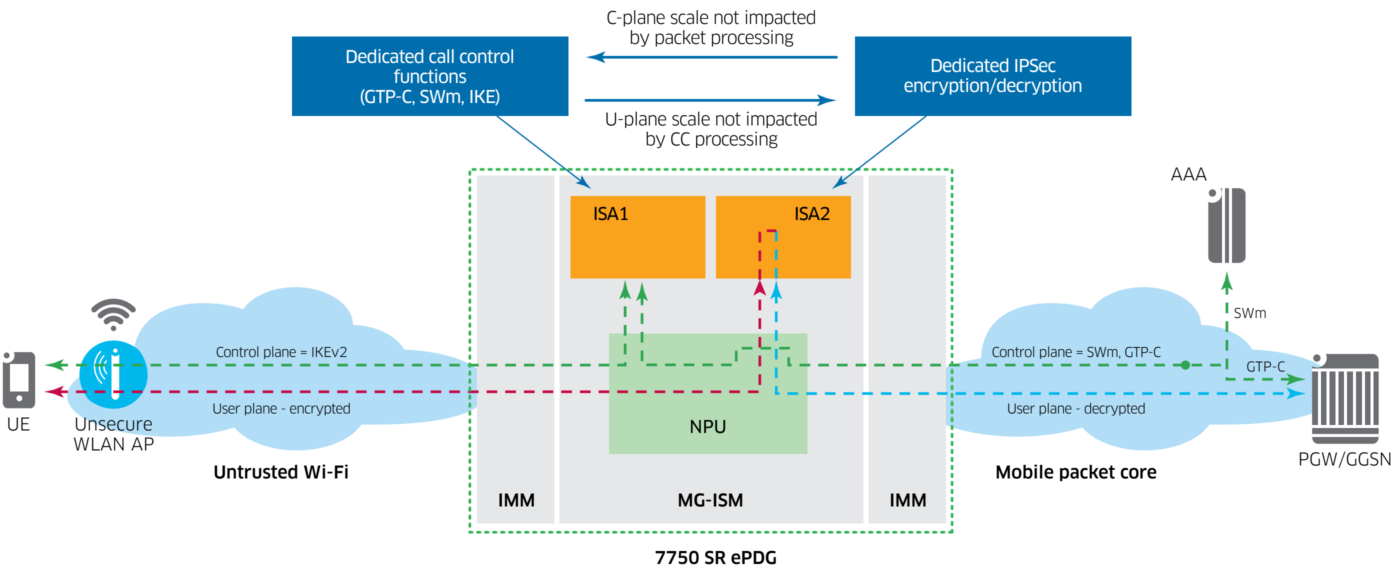


IPSEC PROCESSING WITH PREDICTABLE PERFORMANCE AND SCALE

The ePDG’s role in ultra-broadband mobile networks will require the ePDG to both terminate large numbers of individual IPSec tunnels and handle hundreds of gigabytes of IPSec throughput. For this reason, scalability in both dimensions is a critical requirement, especially for advanced applications and services. When deployed on the 7750 SR platform, the ePDG leverages its embedded service and application intelligence along with its integrated services modules to support advanced application capabilities.

The Mobile Gateway-Integrated Services Module (MG-ISM) performs the mobile gateway functions while simultaneously supporting the high-touch packet operations for deeper levels of integrated service capabilities, such as IPSec. The MG-ISM uses separate processors for the user plane and data plane, both optimized for their task including, accelerated IPSec processing. This allows resources to scale independently so that the platform can support a mix of device types and applications with predictable MG-ISM scale and performance to ensure the optimal user quality of experience.

Figure 5. MG-ISM delivers predictable performance and scale



As a result, when user-driven IPSec traffic volume increases, the Service Routing Operating System's (SR OS) flexible architecture allows operators to increase the number of MG-ISMs deployed in a 7750 SR platform.

HIGH AVAILABILITY AND OPERATIONS AND MANAGEMENT

High availability, achieved through redundancy, addresses the challenge of growing mobile data volumes over untrusted networks. With subscriber QoE expectations already so high, compromise is not an option over untrusted networks. In response, the ePDG function leverages built-in SR OS redundancy and, when deployed on the 7750 SR MG, the platform delivers stateful inter-node/site and intra-shelf redundancy to deliver best-in-class, high availability.

Meanwhile, redundancy is assured at the card level with the deployment of the MG-ISM stateful intra-chassis redundancy within a 7750 SR platform. Stateful intra-chassis includes synchronization of the subscriber, SWu and SWn sessions, as well as the S2b bearer states. In addition, card switchover does not require external protocol support; nor is it user-equipment aware. As a result, continuity of the user equipment application is maintained.

To further expand high availability, geo-redundant deployment options are supported allowing stateful inter-node/site redundancy, which, when combined with the intra-chassis redundancy, can deliver a very high level of service uptime. To achieve stateful inter-node/site redundancy, 7750 ePDGs are deployed as primary/secondary node pairs. Between these ePDG pairs, subscriber SWu and SWn sessions and S2b bearer states are synchronized between the primary and secondary nodes, such that in the event of primary ePDG failure/isolation, the secondary ePDG has all relevant subscriber data to assume responsibility for all currently active sessions. This stateful inter-node/site redundancy synchronization includes user equipment state information, such as Security Associations (SA), encryption keys and the Security Parameter Index (SPI), along with IPSec IKEv2 parameters.

A master-slave arrangement between the two ePDGs, tied to the routing advertisements, assures that the user engagement session, along with the PGW S2b bearer, is maintained. The application of these stateful inter-node/site and intra-chassis redundancy features is further extended by the existing mobile gateway redundancy features that support ePDG subscribers/bearers.

Integrated OAM capabilities for the Alcatel-Lucent mobile gateway functions, (including the ePDG) and for the underlying mobile backhaul and transport networks are delivered by the Alcatel-Lucent 5620 Service Aware Manager (SAM). Its capabilities enable:

- Increased service deployment agility through automation
- Proactive monitoring and management across multiple network layers
- Integration into existing BSS/OSS through flexible and open APIs

INTEGRATED ADVANCED GATEWAY CAPABILITIES

The ePDG supports a wide range of integrated advanced gateway capabilities, including:

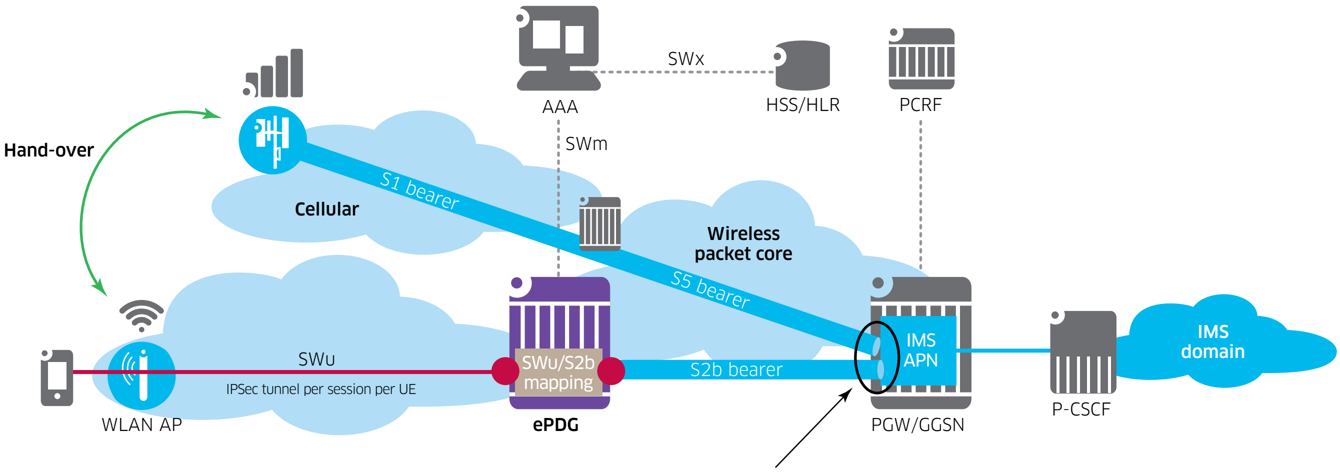
- Dual-stack IPv4 and IPv6 for both network infrastructure and high-scale subscriber support
- Lawful Intercept at high scale and bandwidth for untrusted non-3GPP access subscribers
- Policy interfaces, such as Diameter
- Carrier-grade Network Address Translation (NAT)) for easy use of private network addresses
- Subscriber accounting with the support of Charging Data Record (CDR) or diameter-based records

Furthermore, application assurance (AA) on the ePDG extends the service depth by enabling visibility and intelligent control for IP applications. This includes extensive per-application, per-subscriber, or per service policies, as well as the ability to support Selective IP Traffic Offload (SIPTO) local breakout as operators look to evolve service and deployment models.

MOBILITY BETWEEN RADIO ACCESS TECHNOLOGIES

An additional challenge faced by operators is the need to ensure service and application continuity as well as mobility between untrusted, non-3GPP networks and their cellular infrastructure. To prevent service interruption or degradation, some applications may require IP address continuity as they transition across the Radio Access Types (RATs). To achieve continuity, as illustrated in Figure 5, the ePDG obtains the user equipment IP address from the mobile core so that a common IP address can be assigned to the user equipment. This assignment ensures the preservation of the user equipment IP address on an untrusted, non-3GPP network or as the user equipment moves between the untrusted non-3GPP network and the cellular network.

Figure 6. Continuity and mobility between radio access types

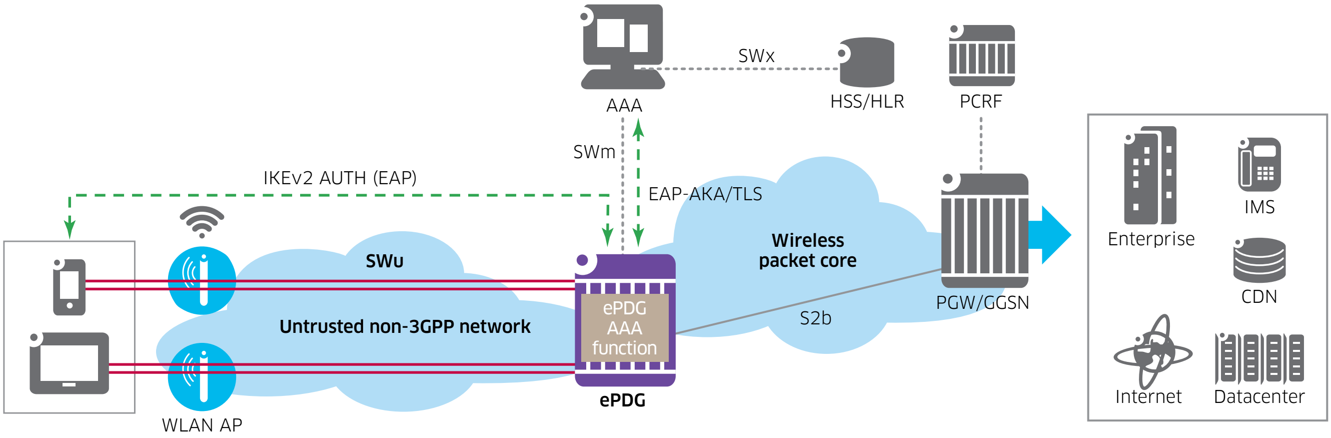


The hand-over signaling triggers the PGW/GGSN to assign the same IP@ to the UE. This allows specific applications to maintain continuity across RAT-type.

AUTHENTICATION FLEXIBILITY

The 7750 SR MG with the ePDG function also supports an extensible set of authentication capabilities. Once authenticated by the operator's AAA server, these capabilities grant secure client access. The 7750 SR ePDG function goes beyond the 3GPP standard to offer authentication for not only SIM-enabled devices but also non-SIM devices, as illustrated in Figure 6. This includes EAP-AKA authentication for SIM-enabled devices, and EAP-TLS authentication for non-SIM-enabled devices. This enables secure access (i.e., authenticated and confidential access) while preserving data integrity for the applications and services delivered by the mobile core via an untrusted, non-3GPP network.

Figure 7. Multiple authentication options



FLEXIBILITY TO GROW AND EVOLVE

Expanding the mobile network in order to support an escalating volume of user sessions across increasingly diverse service types requires delivery across an expanded range of radio access technology (RAT) types. Mobile gateways need to adapt to support this growth and technology diversification while also ensuring that packet processing performance, (which is directly tied the user experience), is maintained.

As exemplified by its multi-dimensional scalability, the 7750 SR is built for scalability and growth of packet processing demands. Because the 7750 SR platform supports a wide range of mobile gateway functions, performance remains unaffected as the platform is pushed to its documented limits (i.e., on the number of bearer channels, throughput, service data flows (SDFs) and other parameters).

As competitive forces mandate service ubiquity and differentiation, the industry is starting to look at flexible resource allocation leveraging standard platforms with Network Function Virtualization (NFV) and cloud architectures being explored as an alternative network evolution path. The 7750 SR MG platform supports the path to virtualization while increasing scalability and evolving to meet 3GPP gateway requirements. This capability enables network evolution to a virtualized, cloud-based architecture at the operator's own pace while also assuring that existing mobile gateways meet performance and scalability requirements for years to come.

CONCLUSION

Competitive and business requirements are motivating operators to deliver secure mobile broadband services over untrusted, non-3GPP networks. However even with the continued expansion of Wi-Fi access, subscribers expect to have the same QoE over untrusted networks as they have over trusted, 3GPP access networks. With the ePDG function, Alcatel-Lucent is partnering with leading operators to meet this challenge. The ePDG supports non-3GPP access, providing seamless delivery of evolved packet core services over untrusted networks, such as residential, public and enterprise Wi-Fi hotspots.

The Alcatel-Lucent ePDG is built upon the highly robust, industry-proven Alcatel-Lucent mobile gateway software, which delivers mobile services with exceptional performance and scale. The ePDG addresses key operator considerations such as scalability, security, user equipment session continuity, high availability, extensible authentication, network integration flexibility and leverages the end-to-end service, aware management capability of the 5620 Service Aware Manager (SAM).

GLOSSARY

3GPP	Third Generation Partnership Project
5620 SAM	Alcatel-Lucent 5620 Service Aware Manager
7750 SR	Alcatel-Lucent 7750 Service Router
7750 SR MG	Alcatel-Lucent 7750 Service Router Mobile Gateway
AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
APN	Access Point Network
BSS	Business Support Systems
CDR	Charging Data Record
CRM	Content Rights Management
EAP	Extensible Authentication Protocol
EAP-AKA	Extensible Authentication Protocol – Authentication Key Agreement
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
ePDG	Evolved Packet Data Gateway
GGSN	Gateway GPRS Support Node
GW	Gateway
IP	Internet Protocol
IPSec	IP Security
LTE	Long Term Evolution
MG-ISM	Mobile Gateway-Integrated Service Module
MGW	Mobile Gateway
NAT	Network Address Translation
NFV	Network Function Virtualization
OAM	Operations, administration and management
OSS	Operations Support Systems
PDN	Packet Data Network
PGW	Packet data network gateway
QoE	Quality of Experience
RAT	Radio Access Type
S2b	3GPP defined GTPv2 reference point
SDF	Service Data Flows
SGW	Serving Gateway
SIPTO	Selective IP Traffic Overload
SWu	3GPP Defined IPsec tunnel reference point
SWm	3GPP Defined AAA reference point
SR OS	Alcatel-Lucent Service Router Operating System
TWAG	Trusted Wireless Access Gateway
TWAP	Trusted WLAN AAA Proxy
WLAN	Wireless Local Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network