Table of Contents

General Description 3

- ***Audience*** 3
- ***Main Functions*** 3

General Description

EPDG Overview on YouTube:

Audience

This guide is intended for employees of mobile telecommunications operators (hereinafter referred to as Operators) responsible for the installation, configuration, maintenance, and monitoring of information systems. Knowledge of data transmission network technologies, Wi-Fi, Long Term Evolution (LTE), and 3G is required.

Main Functions

- Support for SWu interface based on IPsec/IKEv2 between ePDG and WLAN UEs;
- Support for SWm interface based on Diameter between ePDG and external 3GPP AAA server for authentication, re-authentication, fast authentication, and multiple concurrent UE-PDN sessions;
- Packet routing between WLAN UEs and Packet Data Network Gateway (PGW) via the S2b interface using the GTPv2 protocol;
- Support for handover from Wi-Fi to LTE and from LTE to Wi-Fi via the S2b interface;
- Support for dynamic selection of PGW via DNS client, including topology- and weight-based selection. Selection based on topology and weight, as well as AAA, SRV, and S-NAPTR records to ensure connection to the Packet Data Network (PDN) for WLAN UE connectivity;
- Support for emergency calls when the LTE network is unavailable, and UEs either have an authenticated IMSI, unauthenticated IMSI, or no IMSI;
- Support for emergency services based on Access Point Name (APN) configuration for emergency services and IKE tunnel IP address and port information sent via the S2b interface and SWm interface to the 3GPP AAA server;
- Authentication and authorization support for IPsec/GTPv2 tunnels via Extended Authentication Protocol - Authentication and Key Agreement (EAP-AKA) between the 3GPP AAA server and WLAN UEs;
- Support for Layer 2 Tunneling Protocol (L2TP) via Extended Authentication Protocol - Generic

Token Card (EAP-GTC) to support Virtual Private Networks (VPNs) or Internet service providers using Layer 2 Tunneling Protocol (L2TP) tunnels;

- Supports Public Key Infrastructure (PKI) authentication used for exchanging digital certificates between UE and ePDG, including local and intermediate trust certificates between UE and ePDG, including local, ca-trust, and intermediate trust types of certificates. PKI authentication is supported with and without Online Certificate Status Protocol (OCSP) response;
- Supports Certificate Management Protocol (CMPv2) for online registration, update, and revocation of X.509 certificates as described in RFC 4210, RFC 4211, RFC 6712, and 3GPP TS 33.310;
- Support for redundancy;
- Supports buffering of packets to the subscriber until session completion.