Real Time Communication

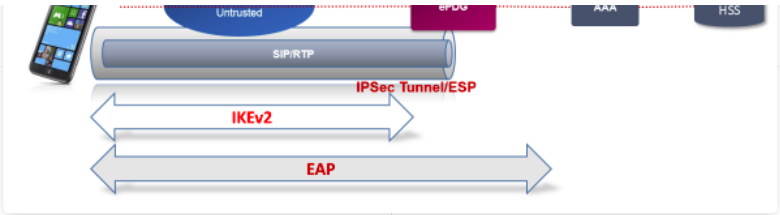
4G/5G, VoLTE, RCS, IMS, SIP, WebRTC, IoT/M2M for engineers

ePDG and IPSec

Posted on April 6, 2016 by realtimecommunication.info

It seemed that once we have IMS in place we can add the VoWifi service for free. Of course, there is hardly ever anything for free. As we have is in the VoWifi Overview there are quite a few things we need to take into account. In IMS we have to be more sensitive when it comes to routing, forking, location services etc. In the access network we have to make sure that the communication is secure enough and that we can trigger an access transfer when needed. In this post we'll go through the security part of it and describe the basic flows.

It is not that difficult to get lost among all the security frameworks, protocols and procedures we have implemented in ePDG. In order to establish an IPSec tunnel we have to use IKEv2 for encryption and then some form of EAP for authentication and then we can start with ESP encryption.



Security over SWu

So let's start with a short dictionary:

IPSec

As defined in the previous post it is a protocol *suite* for a secure Internet Protocol (IP) communication providing authentication and encryption of IP packets. IPSec supports two modes – tunnel and transport. In case of ePDG we'll talk only about the tunnel mode.

IKE

Internet Key Exchange (IKEv2) is a protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. The v2 has some important enhancements which are more or less a must for a network element connected directly to the public Internet. The IKE is described in the RFC 4306 and RFC 5996.

D–H

Diffie–Hellman key exchange is a method for a secure exchange of cryptographic keys over a public channel.

EAP

Extensible Authentication Protocol is an authentication framework providing the transport and usage of keying material and parameters generated by EAP methods. There are cca 40 methods, from which the most important (HotSpot 2.0) for us are:

- EAP-SIM (2G)
- EAP-AKA (3,4G)

- EAP-AKA' (3, 4G)
- EAP-TLS (no SIM)
- EAP-TTLS (no SIM)

Which one is used depends on the capabilities of a client (e.g. if does have a SIM card) and on what is supported by the network. The EAP is defined in RFC 3748 and was updated by RFC 5247.

EAP authentication goes between the UE and AAA.
IKEv2 supports the EAP and handles the establishment of unicast security associations (phase 2a in RFC).

ESP

Encapsulating Security Payload is a protocol within the IPSec protocol suite which provides authentication, integrity and confidentially of IP packets. As we have seen previously, in a tunnel mode the entire packet is encapsulated within another packet as a payload and it is encrypted by ESP.

FLOW

Where to start? Firstly the UE has to discover the ePDG node. Based on operator preference either static ePDG IP addresses or FQDN can be configured on UE. Typically we use FQDN, in that case it must be resolvable within the public Internet. The DNS query is done on the Wi-Fi Internet connection using configured Public DNS IP Address.
The FQDN format is

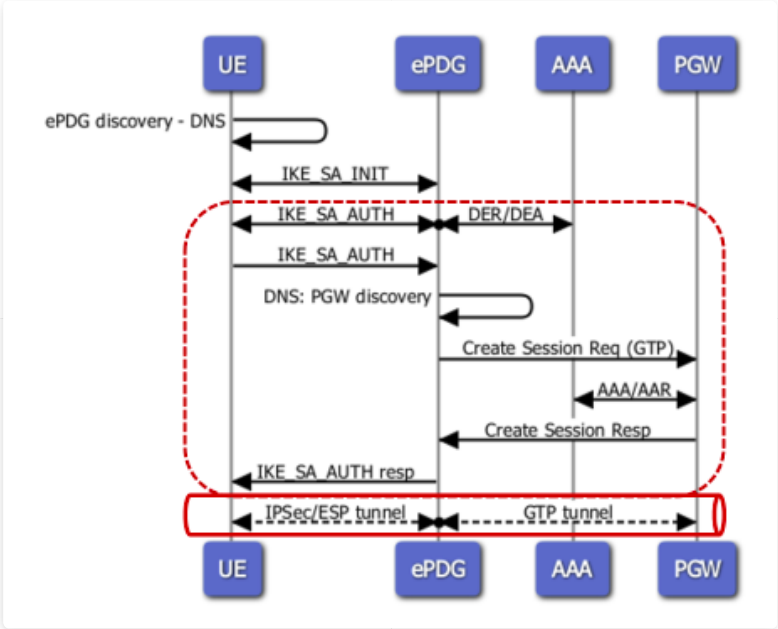
```
epdg.epc.mnc000.mcc000.pub.3gppnetwork.org
```

The UE shall keep using the same ePDG as long as it is reachable. If the connectivity is lost, the UE starts using another ePDG IP address (either configured or provided by the DNS).

Recent Posts

Rate Limit and Traffic Shaping
News: 5G – is our health the toll to pay?
AR, VR – Real-time communication in 5G
News: Wireshark is 20!
Comment: Real-time communication & AI
SIP URI Overview
VoLTE Conference Call
News: Bitcoin and Mobile Networks?
News: RTC in 2017
Multimedia in VoLTE
News: Mobile IoT Deployments
VoIMS – IMS and 5G
VoLTE Flows and CS Network
VoLTE KPIs
News: Trends in Telco
VoLTE Flows – Basics
Comment: A Piece of Advice for Every (Telco) Company
IMS Centralized Services – Overview
NEWS: Number Portability & ENUM
SIP Illustrated 5: SIP Session Routing
SIP Illustrated 4: SIP Session
SIP Illustrated 3: Routing and IMS Registration
SIP Illustrated 2: SIP Message
SIP Illustrated 1: Basics
GSMA Advanced Messaging – RCS Universal Profile
News: 2016 Summary
News: Finally 4G?
News: Telco Monitoring
News: RCS Reborn?
SCTP Introduction
Challenges of Automated Testing (for telcos)
News: IoT and Automatic Emergency Calls

Note, that it is more complex in case of roaming support. Details can be found in GSMA IR.61, 3GPP TS 23.003.



ePDG Flow

The UE must establish a separate SWu instance (i.e. a separate IPsec tunnel) for each PDN connection. The IPsec tunnel transports the packets of all S2b bearer(s) for the same PDN Connection between the UE and the ePDG. The ePDG must release the SWu instance when the default S2b bearer of the associated PDN connection is released.

The UE and ePDG start to communicate over IKEv2. IKEv2 has only two initial phases of negotiation:

- IKE_SA_INIT Exchange
- IKE_AUTH Exchange

IKE_SA_INIT Exchange

IKE_SA_INIT is the initial exchange in which the peers establish a secure channel via D-H. After they finish the initial exchange, all further communication is encrypted.

This first exchange has to be completed before any further exchanges can happen. It performs three functions in the setup of the IKE-SA:

Diameter Overview
OTT and VoLTE Calls
News: UAVs and LTE
IMS Presence Illustrated: Beginners Guide
News: testRTC Demo
News: The World is to be All-IP
VoLTE Illustrated: Beginners Guide
News: IoT and SIM – does it go together?
Rainy-day Scenarios – S-CSCF Restoration
News: Internet in Vivo
How to read Initial Filter Criteria
News: more than HD
ePDG and IPSec
News: WhatsApp pushes the WebRTC
Thanks for your visit!
News: Top 10 IoT Technologies
News: IoT @ home
News: WebRTC – the way to go

Categories

5G (6)
IMS (48)
IoT (10)
LTE (13)
Messaging (3)
OTT (5)
Whatsapp (3)
RCS (27)
IPSMGW (5)
Presence (6)
Uncategorized (22)
VoLTE (39)
VoWifi (11)
WebRTC (15)

Archives

February 2019 (1)
December 2018 (1)
September 2018 (1)
July 2018 (2)
May 2018 (1)
March 2018 (1)

- Negotiation of security parameters for the IKE-SA
- Sends nonces
- Sends D-H values

Note – the form of IKE_SA_INIT is designed in IKEv2 (in contrast to v1) to be more robust enough against the DOS attacks. There are also other improvements of v2 related to MOBIKE support, NAT Traversal, SCTP support, etc.

IKE_AUTH Exchange

After the IKE_SA_INIT exchange is complete, the IKEv2 SA is encrypted. Anyway the remote peer has not been authenticated yet. The IKE_AUTH exchange is used to authenticate the remote peer and create the first IPsec SA.

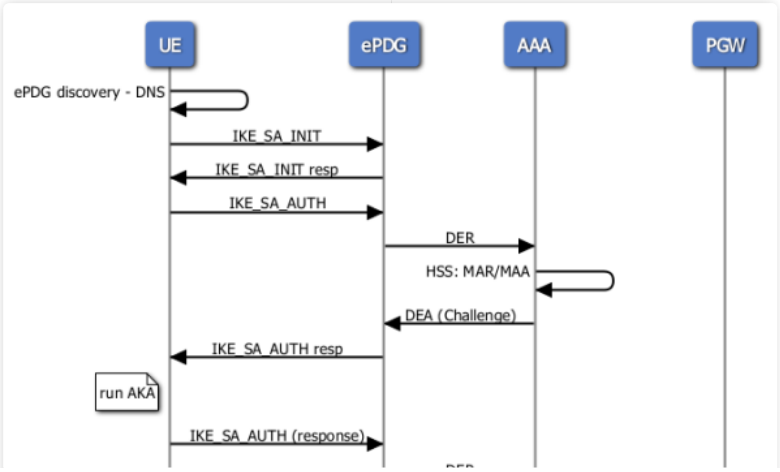
It performs three required functions:

- Transmition of identities
- Proves knowledge of the secrets related to those identities
- Establishment of the ESP

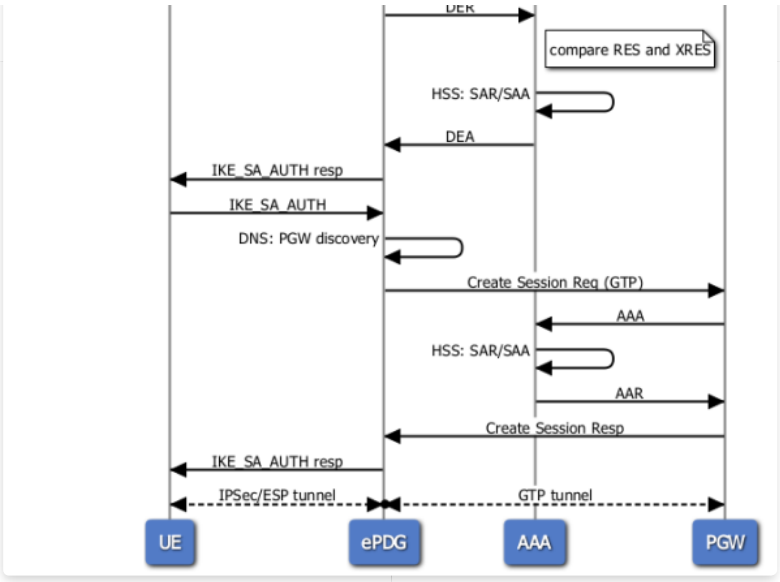
EAP Authentication

Basically we distinguish whether or not the UE is able to access the ISIM/USIM modules. For the clients equipped with the SIM card we use the AKA algorithm. For the others we can use EAP-TLS or EAP-TTLS.

The full IKE/EAP-AKA/ESP flow then can look like this:



January 2018 (2)
December 2017 (1)
November 2017 (1)
October 2017 (4)
September 2017 (1)
August 2017 (1)
May 2017 (2)
March 2017 (2)
February 2017 (3)
January 2017 (2)
December 2016 (3)
November 2016 (1)
October 2016 (1)
September 2016 (1)
August 2016 (2)
July 2016 (2)
June 2016 (4)
May 2016 (2)
April 2016 (3)
March 2016 (5)
February 2016 (2)
January 2016 (2)
November 2015 (5)
September 2015 (3)
July 2015 (1)
June 2015 (4)
May 2015 (3)
April 2015 (1)
March 2015 (8)
January 2015 (3)
December 2014 (7)
November 2014 (5)



IPSec establishment – EAP-AKA

The IKE or IPSec SAs use secret keys should be used for a limited time and to protect a limited amount of data. This is because we want to make sure that even if an attacker finds out the secret keys (e.g by using some brute force mechanism) the amount of data compromised is limited. After the IKE or IPSec SAs is expired a new security association is established to take place of the expired one. The process is known as “Rekeying”.

The rekeying process could be triggered based on duration or amount of data transferred on existing IPSec tunnel and can be initiated by both ePDG or IKEv2 peer. The rekeying is done using a CREATE_CHILD_SA exchange. If both the IKE and IPSec Security association require rekeying then they are performed separately.

For EAP-SIM/AKA/AKA’ we have an optional but important optimization called *fast re-authentication.* It is defined by the GSMA IR.61 and TS 33.402. It provides authentication that does not require new vectors from the HLR/HSS. The original master session key (MSK) from the full authentication is used to generate a fresh MSK. That means that the new triplets from the HSS are not necessary. The UE uses the fast re-authentication identity returned by the AAA. Naturally, the fast re-authentication reduces the load on the HLR/HSS.

Share this:

Loading...

This entry was posted in VoWifi and tagged EAP, EAP-AKA, ePDG, ESP, IKEv2, IPSec. Bookmark the permalink.

← News: WhatsApp pushes the WebRTC

News: more than HD →

8 thoughts on “ePDG and IPSec”

Bien says:

March 5, 2018 at 11:40

Hi,

I am implementing one thing that related to ESP, do you know the way to decrypt a ESP message?

Tks,
/Bien

★ Like

↪ Reply

tttrainer says:

March 5, 2018 at 13:55

Hello Bien,
I doubt I can help you much, there are so many things we have to take into account and I'm not an expert in this area. IPsec provides plenty of options when it comes to encryption. Typically used algorithms are DES, 3DES, Blowfish and AES, to name just a few. Before exchanging data the hosts have to agree on what particular algorithm will be used to encrypt the IP packets and what hash function will be used to ensure the data integrity (e.g. MD5 or SHA). So this is something you have to know before you'll start with the decryption. Btw. I wonder that you're interested only in decryption of the messages, not encryption at the first place. Sounds like an eavesdropping project 🙂

Kind Regards,
Karel.

★ Like

↪ Reply

Johanny says:

March 14, 2018 at 18:52

hi Karel

We are deploying VOWIFI now and customer has requested use and external FW for SWU and configure here the SWU public IP, then FW NAT this ip and

reach the ePDG SWU IP (in this case private IP)…..do you know if this is possible?

In Fac, what customer asked is set the ipsec tunnel only between UE and FW. in order FW can inspect payload information inside the tunnel.

Thanks

★ Like

↪ Reply

tttrainer says:
March 15, 2018 at 08:10

Hello Johanny,
In general I can imagine FW in front of the ePDG. In that case you have to make sure that all the IPs are correctly provisioned. There can be also issues related to access transfer scenarios – as UE is not directly connected to eDPG, you have to have direct 1:1 mapping between eDPG and FW. (FW should be ideally just a *transparent* frontend for ePDG which filters out all IPSec traffic for ePDG.)
To terminate IPSec in FW goes in my view directly against the basic VoWifi idea. E.g. how does FW retrieves the key material?
In case of a good ePDG product there should be no need of any DPI provided by an external FW. ePDG typically has an embedded firewall along with plenty of advanced security features (DDoS protection, traffic shaping, protocol fuzzing etc.). FW with NAT can even make things worst (it would be more difficult to detect/suppress attacking IPs).
Without knowing the details I'd suggest to explain the customer the security functionalities provided by ePDG and check, if there is any real gap covered by their FW only.

Kind Regards,
Karel.

★ Like

↪ Reply

Tsvetan Filev says:
June 26, 2018 at 08:52

Hi.

First of all thanks for the good article.

I'm working on an ePDG implementation and I'm trying to understand how thing are happening on the client side(UE) in order to test how thing work. You wrote the following "Firstly the UE has to discover the ePDG node. Based on operator preference either static ePDG IP addresses or FQDN can be configured on UE.".

I tried to find some android and ios settings to specify FQDN but is seems there is no such setting. I could install external app and make a vpn connection using ikev2 eap-aka but this does not look very native. Do you know if I need some special version of Android for this ?
Is it part of the OS at all ?

Regards.

★ Like

↪ Reply

Realtimecommunication.info says:

June 26, 2018 at 11:16

Hi Tsvetan,
there are in general two ways how to use epdg. Either you're using a native embedded application (true VoWifi) – then the parameters are taken from ISIM/USIM. Or you can use an application running in andriod/ios – here it might be possible to overwrite the FQDN. 3rd party applicactions are usually more demanding when it comes to battery. They are used mainly on SIM-less devices. Honestly I haven't used one for some time already.
Karel.

★ Like

↪ Reply

Joel says:

August 10, 2018 at 09:47

Hi, we are planning to build a UE prototype using ISUM/USIM. Are the applications available to create a UE WiFi calling app that is native that can connect to exsitng ePDG of a mobile network?

★ Like

Realtimecommunication.info says:

September 4, 2018 at 08:45

Hello Joel,
not to my knowledge (but I'm not UE expert). Either we talk about the native client, that one is connected to ePDG. Or some 3rd party app, which is connected over the public Internet directly to the SBC. It's not just the point of connectivity but the whole mechanism of bearer and access transfer control we need to take into account. Sure technically possible is anything.
Karel.

★ Like

Leave a Reply

Enter your comment here...