ENHANCEMENTS TO SERVING A USER EQUIPMENT IN A VISITED COUNTRY IN A MOBILE COMMUNICATION SYSTEM

The present invention generally relates to mobile communication networks and systems.

Descriptions of mobile networks and systems can be found in the literature, such as in particular in Technical Specifications published by standardization bodies such as for example 3GPP (3rd Generation Partnership Project).

An example of 3GPP mobile system is EPS (Evolved Packet System). In a system such as EPS, a User Equipment UE has access to a an EPS network providing communication services (including providing IP connectivity). The EPS network comprises a Core Network called EPC (Evolved Packet Core) that can be accessed not only by 3GPP access, but also by non-3GPP access. A typical example of non-3GPP access, which will be considered more particularly in the following, is WLAN access.

WLAN access to EPC is specified in particular in 3GPP TS 23.402 and 3GPP TS 24.302. In the case of untrusted WLAN access, an IPsec tunnel is established between the UE and an evolved Packet Data Gateway ePDG, to ensure that the UE and the network can communicate in a secure way. The procedure for selection of an ePDG by the UE is specified in particular in 3GPP TS 23.402 and 3GPP TS 24.302.

It is important that an appropriate ePDG is selected for untrusted WLAN access to EPC. As recognized by the inventors and as will be explained with more detail later, the procedure for selection of an ePDG by the UE, as currently specified, needs to be improved.

In particular, there is a need to improve the selection of a ePDG in a country a User Equipment UE is located.

There is also a need to improve the determination of the local emergency numbers in a country a User Equipment UE is located.

More generally, there is a need for enhancements to serving a User Equipment UE in a visited country in a mobile communication system.

Embodiments of the present invention in particular address such needs.

These and other objects are achieved, in one aspect, in some embodiments, by a User Equipment UE, configured to:

- get ePDG selection information configured by the UE's HPLMN, said ePDG selection information including a list of PLMNs with an indication of whether the selection of an ePDG in a PLMN is preferred or mandatory or non-preferred,

- perform selection of an ePDG operated by a PLMN of a country the UE is located in, referred to as local PLMN, which has roaming agreement with the UE's HPLMN for

untrusted WLAN access to EPC, based on said list of PLMNs configured in said ePDG selection information, and on a list of MCCs of said country and/or a list of local PLMNs.

These and other objects are achieved, in another aspect, in some embodiments, by a User Equipment UE, configured to:

- get a list of PLMNs, referred to as local PLMNs, of a country the UE is located in,
- perform selection of an ePDG operated by a local PLMN having roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC, based on said list of local PLMNs, and on information, referred to as local PLMN roaming agreement information, indicating if a local PLMN has roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC.

These and other objects are achieved, in another aspect, in some embodiments, by a User Equipment UE, configured to:

- get a list of PLMNs, referred to as local PLMNs, of a country the UE is located in, which have roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC,
- perform selection of a ePDG operated by a local PLMN having roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC, based on said list.

These and other objects are achieved, in another aspect, in some embodiments, by a DNS Server, configured to:

- receive a DNS query targeting a FQDN including a MCC of a country,
- provide in response a list of identities, MCC and MNC, of PLMNs of said country.

These and other objects are achieved, in another aspect, in some embodiments, by a DNS Server, configured to:

- receive a DNS query targeting a FQDN including:
    - the MCC and MNC of a local PLMN in a UE's visited country, and
    - the MCC and MNC of the UE's HPLMN,
- provide in response a failure indication if said local PLMN has no roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC.

These and other objects are achieved, in another aspect, in some embodiments, by a DNS Server, configured to:

- receive a DNS query targeting a FQDN including:
    - the MCC and MNC of a UE's HPLMN, and
    - a MCC of a country the UE is located in,

- provide in response a list of identities, MCC and MNC, of the PLMNs of said country, which have roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC.

These and other objects are achieved, in another aspect, in some embodiments, by a method for selection of an evolved packet data gateway in a country a User Equipment UE is located, comprising at least one step performed by at least one of a thus configured UE or DNS server.

These and other objects are achieved, in another aspect, in some embodiments, by a DNS Server, configured to:

- receive a DNS query targeting a FQDN including a MCC of a country,
- provide in response a list of emergency numbers of said country.

These and other objects are achieved, in another aspect, in some embodiments, by a P-CSCF, configured to:

- retrieve from a DNS server, based on the MCC of the VPLMN serving an UE, the list of emergency numbers defined in the country corresponding to that MCC

These and other objects are achieved, in another aspect, in some embodiments, by a method for the determination of the local emergency numbers in a country a User Equipment UE is located, comprising at least one step performed by at least one of a thus configured P-CSCF or DNS server.

Some embodiments of apparatus and/or methods in accordance with embodiments of the present invention are now described, by way of example only, and with reference to the accompanying drawings, in which:

- Figure 1 is intended to illustrate, in a simplified way, an example of information used for ePDG selection according to first embodiments of the invention,
- Figure 2 is intended to illustrate, in a simplified way, an example of information used for ePDG selection according to second embodiments of the invention,
- Figure 3 is intended to illustrate, in a simplified way, an example of information used for ePDG selection according to third embodiments of the invention.

Abbreviations

DNS Domain Name System

EPC Evolved Packet Core

ePDG	Evolved Packet Data Gateway
EPS	Evolved Packet System
FQDN	Fully Qualified Domain Name
HPLMN	Home PLMN
IMS	IP Multimedia Subsystem
MCC	Mobile Country Code
MNC	Mobile Network Code
P-CSCF	Proxy Call Session Control Function
PLMN	Public Land Mobile Network
UE	User Equipment
VPLMN	Visited PLMN
WLAN	Wireless Local Area Network

Description of various aspects and/or embodiments of the invention

When a WLAN capable UE is attached via 3GPP access to a 3GPP RPLMN (HPLMN or VPLMN), it is specified according to TS 23.402 clause 4.5.4 (see version v13.4.0) that the UE selects an ePDG in that RPLMN or in its HPLMN.

When the UE is not attached via 3GPP access to a 3GPP PLMN, it is specified that the UE shall select an ePDG in the country it is located in by constructing a corresponding Operator Identifier FQDN (with MCC and MNC as specified in TS 23.003). But a condition is that the selected PLMN shall be in the “ePDG selection information” (see 4.5.4.4 bullet 2)a)), which does not include all the PLMNs that have roaming agreements for untrusted WLAN with the UE's HPLMN but only the mandatory and preferred PLMNs (i.e. the local PLMNs for which the HPLMN has decided it is mandatory or preferred that the UE selects an ePDG in that PLMN). That “ePDG selection information” has been previously provided to the UE by its HPLMN.

For Lawful Interception, local country regulation authorities may mandate that a UE in the country must select an ePDG in that country. In that case the algorithm to select an ePDG must remain independent from information from other countries. This includes not relying on the “ePDG selection information” because this information is provided by the HPLMN (and may contradict the requirement to select an ePDG in the visited country).

Another use case when the UE must select an ePDG in the same country it is located in is for emergency calls via WiFi when the UE is not attached to any 3GPP PLMN.

In some embodiments:

The UE is assumed to be able to determine the country it is located in. The idea is to enable a WLAN capable UE to get via new additional information in the ePDG selection information and/or via one or more DNS queries, a list of "local" PLMN's (i.e. PLMN's that are in the country the UE is located in) which have roaming agreements for untrusted WLAN access with the UE's HPLMN i.e. that own one or more ePDGs that can authenticate and authorize UE(s) from the HPLMN of the UE.

The DNS servers are public (accessible from anywhere on the Internet).

With the knowledge of local PLMN's having roaming agreements for untrusted WLAN access with the UE's HPLMN, the UE can attempt to establish an IPSec tunnel per TS 24.302 subclause 7.2.2 to an ePDG that is operated by one of these PLMN's.

Three alternatives, referred to as Alternative 1, Alternative 2, Alternative 3, may be distinguished.

Embodiments and/or aspects of the invention related to these different alternatives may be described in the following way.

Alternative 1

One alternative is to extend the attributes of each PLMN in the ePDG selection info "mandatory, preferred" with "not preferred". This allows knowing which PLMNs have roaming agreements with the UE's HPLMN.

In this alternative, either the UE already knows the list of MCCs of the country it is located in, or it needs to query a public DNS to get the full list of PLMNs (MCC and MNC) of the country. The corresponding DNS records are managed by a central administration

The input is a FQDN which includes the MCC (or one of the MCCs) of the country the UE is located in. The output is the list of the identities of the PLMN's of the country (MCC and MNC). The Resource Record is a NAPTR record.

Then the UE attempts to establish an IPSec tunnel per TS 24.302 subclause 7to an ePDG that is operated by any PLMN in the above list only if the PLMN is configured in the ePDG selection Info.

This alternative implies dependence from the HPLMN because ePDG Selection Info is provided by the HPLMN, but it avoids a subsequent DNS query as in alternative 2. If – due to misconfiguration - a PLMN is not provided by the HPLMN in the ePDG selection info, the UE will just not attempt to select ePDG in that PLMN, but it does not harm because the UE will not attempt to select an ePDG in its HPLMN.

Alternative 2

Similar to alternative 1 but the ePDG selection info is not enhanced with "not preferred". In this case, the UE does not know all the roaming agreements since the ePDG selection info does not contain the "non-preferred PLMNs".

The UE first queries a public DNS to get the list of local PLMNs (MCC and MNC) of the country exactly as in alternative 1 but even if it knows all the MCCs of the country.

There is a need for a second set of (DNS) queries to keep only the list of local PLMN's that have roaming agreements for untrusted WLAN access with the UE's HPLMN (so as to prune out the local PLMN that haven't such agreement within the list of PLMN retrieved by the first query of alternative 1).

This second set of queries corresponds to DNS queries targetting a FQDN which includes:

- The MCC and the MNC of a local PLMN in the visited country;
- The MCC and the MNC of the UE's HPLMN.

The output of the each DNS query on each local PLMN is

- A failure if the local PLMN has no roaming agreements for untrusted WLAN access with the UE's HPLMN;
- an FQDN (that may depend on the UE's HPLMN) that allows to further obtain a list of ePDGs of the local PLMN that can serve users of the HPLMN . This avoids the VPLMN having to configure the list of ePDG IP addresses for each of the HPLMN it has roaming agreement with.

Alternative 3

Another alternative is for the UE to directly query a DNS that returns the list of PLMNs which have a roaming agreement for untrusted WLAN with the UE's HPLMN.

The input of the DNS is a FQDN which includes:

- The MCC and the MNC of the UE's HPLMN;
- The MCC (or one of the MCCs) of the country the UE is located in (it is assumed that the UE can know the country it is located in).

The output of the DNS is a list of the identities (MCC and MNC) of the PLMNs of the country that have roaming agreements for untrusted WLAN access with the UE's HPLMN. That list can be ordered.

This feature is e.g. to be used

- when the UE has received instructions that in the local country where it is currently camping it shall only use ePDG that are local in the country (allowing thus Lawful Interception in the local country)

  or for emergency calls via WLAN.

Embodiments and/or aspects of the invention related to these different alternatives may further be described in the following way.

When a WLAN capable UE can determine the country it is located in and either the UE is attempting to make an emergency call via WiFi or the UE has received instructions that in the country where it is currently camping it shall only use ePDG that are located in the country, and if the UE is not attached via 3GPP access to a 3GPP PLMN (or if the UE has failed to be served by an ePDG of the RPLMN that serves it over 3GPP access), the UE selects an ePDG in a PLMN in this country as follows:

As a first alternative:

1) As a first aspect of the invention, in some embodiments, this alternative assumes that the attribute of each PLMN in the ePDG selection info specified in TS 23.402 (§4.5.4.3) "mandatory", "preferred" is enhanced with the value "not preferred". A "not preferred" PLMN configured in the ePDG selection information is a PLMN for which the selection of an ePDG in the VPLMN is allowed (if the UE is required to select a local ePDG) but for which the selection of an ePDG in the HPLMN is preferred (if the UE is not required to select a local ePDG).
2) The UE detects the country it is located in and determines one of the MCCs of the country (a country may have several MCCs https://fr.wikipedia.org/wiki/Mobile_country_code);
3) As a second aspect of the invention, in some embodiments, the UE optionally (e.g. if it does not know the list of MCCs of the country) tries to get a list of local PLMN's (i.e. a list of PLMNs in the country the UE is located in) by performing a DNS query on an input FQDN containing "mcc<MCC>" to a public NAPTR DNS server that returns a list of FQDN that each contains a "mnc<MNC>.mcc<MCC>" of a local PLMN; The domain of the input FQDN does not correspond to an individual operator as the corresponding DNS record is likely not to be managed by an individual operator (could be managed by GSMA)
4) The UE attempts to establish an IPSec tunnel per TS 24.302 subclause 7 to an ePDG that is operated by any PLMN in the above list only if the local PLMN is configured in the ePDG selection Info (since ePDG roaming is "guaranteed" with the PLMN's in ePDG selection info);

3GPP TS 23.003 provides an informative annex D “Applicability and use of the ".3gppnetwork.org" domain name” that can be used to construct a FQDN. A rule of this annex is that a DNS managed by an operator identified by mnc<MNC>.mcc<MCC> can be reached by an UE by using a FQDN with the form "<service_id>.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org". Hence, a public DNS that is not managed by a specific operator should use another form.

As an example for that alternative, the input FQDN to be used for the DNS query would have the form "mcc<MCC>.local-plmn.pub.3gppnetwork.org", the public DNS server returning a list of "mnc<MNC>.mcc<MCC>.local-plmn.pub.3gppnetwork.org" output FQDNs.

Note that in case multiple MCC values may correspond to the local country, the MCC value in an output FQDN could have a different value than the MCC value in the input FQDN.

An example of information used for ePDG selection by a UE, in embodiments related to the first alternative, is illustrated in figure 1. In figure 1, such information includes ePDG selection information enhanced with non-preferred PLMNs, and may (as illustrated with dotted lines) include a list of local PLMNs, obtained e.g. by DNS query to a public DNS server.

As a second alternative,

1) This alternative assumes that the attributes of each PLMN in the ePDG selection info "mandatory, preferred" are as specified in TS 23.402;
2) Same as step 2) in alternative 1;
3) Same as step 3) in alternative 1 in order to determine a list of local PLMN;
4) The UE attempts to establish an IPSec tunnel per TS 24.302 subclause 7. to an ePDG that is operated by any PLMN in the above list if the PLMN is configured in the ePDG selection Info (since ePDG roaming is “guaranteed” with the PLMN's in ePDG selection info);
5) If there is no PLMN in the list returned by the DNS server that is also indicated in the ePDG selection info, or if the UE did not succeed in establishing an IPsec tunnel to an ePDG in step 4, the UE tries to get a list of local ePDG's having a roaming agreement with its HPLMN:
    a. The UE removes the local PLMN(s) that it has tried to contact at step 3;
    b. For each of the remaining local PLMN(s), the UE performs a DNS query to the local PLMN NAPTR DNS server with an FQDN including the UE’s HPLMN (hmnc<MNC>.hmcc<MCC>) and the local PLMN ID

(mnc<MNC>.mcc<MCC>). Since the DNS is managed by the operator, the FQDN would have a format like "epdg.hmnc<MNC>.hmcc<MCC>.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org". The DNS server returns a substitute FQDN e.g. in a "s" NAPTR record if there is a roaming agreement with the HPLMN, and a rejection otherwise. If the UE "resolver" gets a substitute FQDN from the DNS server, it issues a second DNS request (e.g. SRV type) with the substitute FQDN. The output is a list of IP addresses or a SRV record for ePDG depending on whether the substitute FQDN is associated with an “a” or “s” record.

Step b allows avoiding costly failed IPSec establishment attempts from the UE where the UE tries to contact an ePDG of a local PLMN which has no roaming agreement for untrusted WLAN with the UE's HPLMN (IKE-SA-INIT + Authentication signaling, generally up to the 3GPP AAA proxy which sum up to 6 useless messages).

6) The UE attempts to establish an IPSec tunnel per TS 24.302 subclause 7to an ePDG that is operated by one of these PLMN's.

An example of information used for ePDG selection by a UE, in embodiments related to the second alternative, is illustrated in figure 2. In figure 2, such information includes a list of local PLMNs obtained e.g. by DNS query to a public DNS server, and information noted local PLMN roaming agreement information (indicating if a local PLMN has roaming agreement with the UE’s HPLMN for untrusted WLAN access to EPC) obtained e.g. by DNS query to a local PLMN DNS server.

As a third alternative, the UE selects an ePDG in a PLMN in the country it is located in as follows:

1) The UE detects the country it is located in and determines one of the MCCs of the country;
2) The UE tries to get a list of local PLMNs having an ePDG roaming agreement with its HPLMN by performing a DNS query to a local DNS server with an FQDN including the UE’s HPLMN (hmnc<MNC>.hmcc<MCC>) and the local country MCC (mcc<MCC>) it has determined in step1 (there may be several MCCs in a country). The DNS server returns a list of PLMNs (mnc<MNC>.mcc<MCC>) which have roaming agreements for untrusted WLAN with the UE's HPLMN;
3) The UE attempts to establish an IPSec tunnel per TS 24.302 subclause 7to an ePDG that is operated by one of these PLMN's.

TS 23.003 provides an informative annex D “Applicability and use of the ".3gppnetwork.org" domain name” that can be used to construct a FQDN. As an example, in that third alternative, the FQDN would have the form

"hmnc<MNC>.hmcc<MCC>.mcc<MCC>.lcepdg.pub.3gppnetwork.org", where the service is local country ePDG (lcepdg), the MCC of the country the UE is located in is mcc, and the UE’s HPLMN is hmcc plus hmnc.

The DNS is configured with a list of local PLMN in the country identified by “mcc” the UE's HPLMN has WLAN roaming agreements with. Until successful IPSec tunnel establishment with an ePDG, for each of the local PLMN in the list:

- the UE tries to retrieve the identity of an ePDG of that PLMN as if the UE was registered on that local PLMN (using the Operator Identifier FQDN described in 23.402 §4.5.4.2);
- the UE attempts to establish an IPSec tunnel per TS 24.302 subclause 7.

As an implementation example for the third alternative, the UE fetches the NAPTR record associated with “hmnc<MNC>.hmcc<MCC>.mcc<MCC>.lcepdg.pub.3gppnetwork.org.” The DNS NAPTR information it gets is a set of NAPTR records:

- with the same NAPTR preference and order (to ensure fairness among the operators);
- with the “flags” field set to “a” (as according to IETF RC 3403, "The Application defines the flag ’a’ to mean a terminal lookup and that the output of the rewrite will be a domain name for which an A record should be queried"). Indeed, the DNS resolver in the UE will use the returned FQDN to get the IP addresses of ePDGs;
- not containing any regular expression (“regexp”) for substitution (to avoid complex algorithm in the UE);
- but containing an NAPTR “replacement” field an Operator Identifier FQDN (as defined in 23.402 §4.5.4.2) of a VPLMN that supports ePDG roaming with the HPLMN.

The DNS resolver in the UE then needs to pick an Operator Identifier FQDN and issues a DNS lookup towards that new domain in order to find an ePDG of the corresponding local PLMN.

An example of information used for ePDG selection by a UE, in embodiments related to the third alternative, is illustrated in figure 3. In figure 3, such information includes a list of local PLMNs having roaming agreement with the UE’s HPLMN for untrusted WLAN access to EPC (noted list of PLMNs having roaming agreement), obtained e.g. by DNS query to a DNS server.

For all alternatives, a fair usage of the PLMN (s) in the list can be achieved by the DNS providing the list of local PLMNs using NAPTR records having the same order and same preference (per RFC 34.03 definitions), and the DNS resolver in the UE randomly choosing between the PLMNs for which an IPSec tunnel establishment has not been successfully attempted. Another possibility is that the DNS provides a list of local PLMNs in a random or round robin order and that the UE always start with the first PLMN in the list.

Another need to fulfill is related with a P-CSCF (as defined in 3GPP 23.228) in a Home PLMN (HPLMN) that for IMS services needs to serve an UE located a Visited PLMN (VPLMN) of another country (this scenario is studied as part of S8 Home Routed studies in the FS_V8 SID documented in TR 23.749). In that case the P-CSCF in the HPLMN needs to determine whether session signaling initiated by the UE in the VPLMN targets an emergency number defined in that VPLMN (for example the emergency numbers related with child or women abuse may vary from country to country).

When the session signaling initiated by the UE in the VPLMN targets an emergency number defined in that VPLMN, the P-CSCF in HPLMN has to redirect the UE towards selecting a P-CSCF for emergency services in the VPLMN.

For the purpose of detecting whether session signaling initiated by the UE in the VPLMN targets an emergency number defined in that VPLMN, the P-CSCF could be locally configured with the list of emergency numbers associated with each country of a VPLMN with which it has roaming agreements.

This would be cumbersome to manage.

Another simpler solution would be where the P-CSCF takes the MCC of the VPLMN (where the UE is located) to build a specific FQDN associated with the emergency numbers in that country and issues a DNS record request to get the list of the emergency numbers in that country.

As another aspect of the invention, in some embodiments, the P-CSCF tries to get a list of local emergency numbers (i.e. a list of emergency numbers in the country the UE is located in) by performing a DNS query on an input FQDN containing "mcc<MCC>" (of the PLMN where the UE is camping) to a public NAPTR DNS server that returns a list of such emergency numbers; The domain of the input FQDN does not correspond to an individual operator as the corresponding DNS record is likely not to be managed by an individual operator (could be managed by GSMA like the NAPTR record of the public DNS server that returns a list of FQDN that each contains a "mnc<MNC>.mcc<MCC>" of a local PLMN). The P-CSCF is not assumed to retrieve this list each time an UE registers or issues session related signaling as it may cache the DNS record received as part of DNS look-up

Various aspects and/or embodiments of the invention include (though not being limited to) following aspects and/or embodiments.

Some aspects are related to a User Equipment UE.

Various embodiments may be provided, including (though not being limited to) following embodiments, which may be taken alone or in combination, according to various combinations.

In an embodiment said UE is configured to:

- get ePDG selection information configured by the UE's HPLMN, said ePDG selection information including a list of PLMNs with an indication of whether the selection of an ePDG in a PLMN is preferred or mandatory or non-preferred.

In an embodiment said UE is configured to:

- perform selection of an ePDG operated by a PLMN of a country the UE is located in, referred to as local PLMN, which has roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC, based on said list of PLMNs configured in said ePDG selection information, and on a list of MCCs of said country and/or a list of local PLMNs.

In an embodiment said UE is configured to:

- determine said list of MCCs,

- attempt to establish an IPsec tunnel to an ePDG operated by a PLMN configured in said ePDG selection information, if a MCC of said PLMN is in said list of MCCs.

In an embodiment said UE is configured to:

- get said list of local PLMNs,

- attempt to establish an IPsec tunnel to an ePDG operated by a PLMN of said list of local PLMNs, if said PLMN is configured in said ePDG selection information.

In an embodiment said UE is configured to:

- get said list of local PLMNs, via DNS query to a DNS server on an input containing a MCC of the country the UE is located in.

In an embodiment, said UE is configured to:

- get a list of PLMNs, referred to as local PLMNs, of a country the UE is located in.

In an embodiment, said UE is configured to:

- perform selection of an ePDG operated by a local PLMN having roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC, based on said list of local PLMNs, and on information, referred to as local PLMN roaming agreement information, indicating if a local PLMN has roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC.

In an embodiment, said UE is configured to:

- get said list of local PLMNs, via DNS query to a DNS server on an input containing a MCC of the country the UE is located in.

In an embodiment, said UE is configured to:

- get said local PLMN roaming agreement information, via DNS query to a DNS server targeting a FQDN including:
    - the MCC and MNC of said local PLMN, and
    - the MCC and MNC of the UE's HPLMN,

the output of said DNS query indicating a failure if said local PLMN has no roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC.

In an embodiment, said UE is configured to:

- get a substitute FQDN from said DNS server if said local PLMN has roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC, and issue a second DNS query with the substitute FQDN, to further obtain a list of ePDGs operated by said local PLMN, that can serve users of the UE's HPLMN.

In an embodiment, said UE is configured to:

- get ePDG selection information configured by the UE's HPLMN, including a list of PLMNs with an indication of whether the selection of an ePDG in a PLMN is preferred or mandatory,
- attempt to establish an IPsec tunnel to an ePDG operated by a PLMN of said list of local PLMNs, if this PLMN is configured in the ePDG selection information,
- if there is no PLMN in said list of local PLMNs that is also configured in said ePDG selection information, or if the UE did not succeed in said attempt to establish said IPsec tunnel, get said local PLMN roaming agreement information.

In an embodiment, said UE is configured to:

- get a list of PLMNs, referred to as local PLMNs, of a country the UE is located in, which have roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC.

In an embodiment, said UE is configured to:

- perform selection of a ePDG operated by a local PLMN having roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC, based on said list.

In an embodiment, said UE is configured to:

- get said list via DNS query to a DNS server.

In an embodiment, said UE is configured to:

- perform said ePDG selection if said UE is required to select an ePDG operated by a local PLMN in a country where the UE is located.

Other aspects are related to DNS Server(s).

Various embodiments may be provided, including (though not being limited to) following embodiments, which may be taken alone or in combination, according to various combinations.

In an embodiment, a DNS Server is configured to:

- receive a DNS query targeting a FQDN including a MCC of a country,
- provide in response a list of identities, MCC and MNC, of PLMNs of said country.

In an embodiment, a DNS Server is configured to:

- receive a DNS query targeting a FQDN including:
    - the MCC and MNC of a local PLMN in a UE's visited country, and
    - the MCC and MNC of the UE's HPLMN,
- provide in response a failure indication if said local PLMN has no roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC.

In an embodiment, a DNS Server is configured to:

- provide in response a substitute FQDN if said local PLMN has roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC, said substitute FQDN enabling said UE to get a list of ePDGs of said local PLMN that can serve users of the UE's HPLMN.

In an embodiment, a DNS Server is configured to:

- receive a DNS query targeting a FQDN including:
    - the MCC and MNC of a UE's HPLMN, and
    - a MCC of a country the UE is located in,
- provide in response a list of identities, MCC and MNC, of the PLMNs of said country, which have roaming agreement with the UE's HPLMN for untrusted WLAN access to EPC.

Other aspects are related to a method for selection of an evolved packet data gateway in a country a User Equipment UE is located, comprising at least one step performed by at least one of a thus configured UE or DNS server.

Other aspects are related to a DNS Server.

Various embodiments are provided, including:

In an embodiment, said DNS Server is configured to:

- receive a DNS query targeting a FQDN including a MCC of a country,
- provide in response a list of emergency numbers of said country.

Other aspects are related to a P-CSCF.

Various embodiments are provided, including:

In an embodiment, said P-CSCF is configured to:

- retrieve from a DNS server, based on the MCC of the VPLMN serving an UE, the list of emergency numbers defined in the country corresponding to that MCC

Other aspects are related to method for the determination of the local emergency numbers in a country a User Equipment UE is located, comprising at least one step performed by at least one of a thus configured P-CSCF or DNS server.

A person of skill in the art would readily recognize that steps of various above-described methods can be performed by programmed computers. Herein, some embodiments are also intended to cover program storage devices, e.g., digital data storage media, which are machine or computer readable and encode machine-executable or computer-executable programs of instructions, wherein said instructions perform some or all of the steps of said above-described methods. The program storage devices may be, e.g., digital memories, magnetic storage media such as a magnetic disks and magnetic tapes, hard drives, or optically readable digital data storage media. The embodiments are also intended to cover computers programmed to perform said steps of the above-described methods.

CLAIMS

1. A user equipment, being configured to:

determine a visited country the user equipment is located in,

perform a domain name system query to a DNS server using one or more mobile country codes of the visited country, to obtain, via the DNS server, a list of public land mobile networks located in the visited country, referred to as local public land mobile networks;

select an evolved packet data gateway to establish an internet protocol security tunnel to the evolved packet data gateway from the user equipment, the selecting comprising determining the evolved packet data gateway is operated by one of the local public land mobile networks determined based on the list of local public land mobile networks obtained via the DNS server and on information indicating if the one of the local public land mobile networks has a roaming agreement with a home public land mobile network of the user equipment for untrusted wireless local area network access.

2. The user equipment according to claim 1, being further configured to:

perform the selecting by selecting the evolved packet data gateway operated by the one of the local public land mobile networks of the list, if the one of the local public land mobile networks of the list is configured in evolved packet data gateway selection information provided to the user equipment by the home public land mobile network of the user equipment.

3. The user equipment according to claim 1 or 2, being further configured to:

perform the selecting if the user equipment is required to select an evolved packet data gateway operated by a local public land mobile network in the visited country.

4. A method of operating a user equipment, the method comprising:

determining a visited country the user equipment is located in,

performing a domain name system query to a DNS server using one or more mobile country codes of the visited country, to obtain, via the DNS server, a list of public land mobile networks located in the visited country, referred to as local public land mobile networks;

selecting an evolved packet data gateway to establish an internet protocol security tunnel to the evolved packet data gateway from the user equipment, the selecting comprising determining the evolved packet data gateway is operated by one of the local public land mobile networks determined based on the list of local public land mobile networks obtained via the DNS server and on information indicating if the one of the local public land mobile networks has a roaming agreement with a home public land mobile network of the user equipment for untrusted wireless local area network access.

5. The method according to claim 4, wherein

the selecting the evolved packet data gateway which is operated by the one of the local public land mobile networks of the list is performed by selecting the evolved packet data gateway, if the one of the local public land mobile networks of the list is configured in evolved packet data gateway selection information provided to the user equipment by the home public land mobile network of the user equipment.

6. The method according to claim 4 or 5, further comprising:

performing the evolved packet data gateway selection if the user equipment is required to select an evolved packet data gateway operated by the one of the local public land mobile networks of the list in the visited country.

7. Computer software product including executable software code being stored on a computer-readable medium and, when being executed by means of a processor of a user equipment, carrying out the steps of:

determining a visited country the user equipment is located in,

performing a domain name system query to a DNS server using one or more mobile country codes of the visited country, to obtain, via the DNS server, a list of public land

mobile networks located in the visited country, referred to as local public land mobile networks;

selecting an evolved packet data gateway to establish an internet protocol security tunnel to the evolved packet data gateway from the user equipment, the selecting comprising determining the evolved packet data gateway is operated by one of the local public land mobile networks determined based on the list of local public land mobile networks obtained via the DNS server and on information indicating if the one of the local public land mobile networks has a roaming agreement with a home public land mobile network of the user equipment for untrusted wireless local area network access.

8. Computer software product according to claim 7, including the executable software code being stored on the computer-readable medium and, when being executed by means of the processor of the user equipment, carrying out the steps of the method according to one of the claims 4 to 6.