HAL
open science

Resolving ten MVNO issues with EPS architecture, VoLTE and advanced policy server

Rebecca Copeland, Noel Crespi

To cite this version:

Rebecca Copeland, Noel Crespi. Resolving ten MVNO issues with EPS architecture, VoLTE and advanced policy server. ICIN '11 : 15th International Conference on Intelligence in Next Generation Networks : From Bits to Data, from Pipes to Clouds, Oct 2011, Berlin, Germany. pp.29-34, 10.1109/ICIN.2011.6081093 . hal-00766652

HAL Id: hal-00766652

https://hal.science/hal-00766652v1

Submitted on 18 Dec 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Resolving Ten MVNO Issues with EPS Architecture, VoLTE and Advanced Policy Server

Authors Rebecca Copeland, Core Viewpoint Ltd, Kenilworth, Warwickshire, United Kingdom

Authors Noël Crespi, Institut Telecom, Telecom SudParis, Evry, France

Abstract— **The numbers of MVNOs (Mobile Virtual Network Operator) are growing globally, but so do their operational and business issues. This paper identifies these issues and looks for remedies via the new 4G architecture and interfaces. The paper examines the 'Full' MVNO model as a 'Home' network in a pseudo roaming scenario (National Roaming), allowing MVNO to connect to multiple MNOs through the discovery and selection process, and to benefit from the access agnostic nature of EPS (Enhanced Packet System). Greater MVNO independence can resolve many of the MVNO's underlying issues, e.g. launching services and variable charging that are enabled by IMS Voice and non-Voice. Other persisting issues are solved by the MVNO defining user centric policies that are conveyed to the MNO transport network through new interfaces for the Policy & Charging Rules Function (PCRF). Particular issues can be resolved by integrating the User Data Repository (UDR) with policies and charging rules. MVNO also need to support the value chain via 'Sponsored Data' from service/content providers and receive Traffic Detection Function (TDF) reports on user context and behaviour. This paper argues that these features strengthen the Full MVNO position in the layered business model in EPS, and that the identified issues are substantially alleviated.**

Keywords- Policy, PCRF, MNO, VoLTE, QoS, QoE, LTE, EPC, EPS, IMS, OCS, ePDG, ANDSF, UDR, PMIP.

I. INTRODUCTION

The MVNO Landscape is changing fast with MVNOs implementing numerous models of operating the virtual network. See Ref [8] for classification of MVNO business types. Some MVNOs are part of the MNO organizations, obtaining network capacity internally. Other MVNOs are successful in just reselling the MNO's offerings under their own brand, i.e. no virtual network. This paper does not refer to such cases, but addresses MVNOs who opt for operating part or all of the network core functions.

MVNOs are progressively investing in their own equipment, seeking to gain operational independence. This is not easy for organizations that lack Telecom Mobile networks skills and those who base their business on low margins and low cost base. As LTE (Long Term Evolution) begins to roll out, MVNOs need to consider further what benefits such an upgrade would bring and whether the new technology can alleviate business and technical issues.

In this paper, aspects of the technology are examined against MVNOs' needs. **Part II** details a list of persistent issues that MVNOs have to battle with. **Part III** examines the architectural solutions, including the layered model that allows business autonomy, the National Roaming model for MVNOs. It describes the evolution to LTE for 'thin' and 'full' MVNO. In **Part IV** the main features are examined against the issues list. It argues that EPS (Evolved Packet System), VoLTE (Voice over LTE) and IMS (IP Multimedia Subsystem) offer remedies to these issues and even open up new opportunities. The paper proposes to apply new standard interfaces to the MVNO case, including interfaces to the Policy Server (PCRF - Policy and Charging Rules Function) and the OCS (Online Charging Server). ANDSF (Access Network Discovery & Selection Function), Sponsored Data for SP (Service Provider) and TDF (Traffic Detection Function) for triggering events in the BBERF (Bearer Binding & Event Reporting Function), analyzed in the context of the MVNO. **Part V** contains a summary and a table of issues with their potential remedies.

II. TEN PERSISTENT MVNO ISSUES

MVNOs are 'caught' between customers and suppliers, thus experiencing special middleman difficulties. The following is a compiled list of ten most troublesome MVNOs' issues (excluding the persistent issues of reducing costs) from Ref. [10], [11], [12], [13] plus vendors' white papers and personal quotes from MVNOs in France, Germany and UK:

1) Ability to launch services independently of MNOs: MVNOs must introduce new services frequently and not held back by MNOs' slow pace and traditional approach.

2) Compatibility with MNOs: MVNOs are dependent on the interfaces to MNOs and look to simplify them and avoid high integration costs.

3) Controlling user IDs and accounts data: MVNOs want to issue subscribers SIM cards. They want to avoid disclosure of their subscribers' commercial information and market intelligence to the MNOs.

4) Enforcing Policy remotely: MVNOs need to apply their policies via other networks, e.g. thresholds, restrictions or level of service to be enforced in the MNO transport and access networks.

5) Supporting alternative and untrusted access networks: MVNOs would benefit from utilizing the free WiFi access to reduce their network costs.

6) Detecting user behaviour and context Data: MVNOs want to exploit User intelligence (context and preferences)

for Mobile advertising, and for location-based and transactional services.

7) Variable pricing, credit and quota control: MVNOs must control Prepaid usage 'remotely'. They need to match MNO's usage-based costing to avoid margins erosion.

8) Connecting to 3rd party Service/Content providers and get paid: MVNOs often specialize in delivering content from 3rd parties' with no direct relationships with the MNO. To get paid, MVNOs need to convey service authorization and SP charging across to the MNO.

9) Selecting best alternative access network: To reduce cost, MVNOs can link to several MNOs, choosing the best connection. To do that, MVNOs need to control access networks selection by the handset.

10) Security for non-MNO untrusted access: MVNOs must ensure that untrusted access points do not compromise network and user security.

III. MVNO Architectural Solutions

A. Aligning of Business with Network Layers

Several of the persisting issues stem from MVNOs' dependence on MNOs. While this cannot be entirely avoidable, the evolving networks do support MVNO autonomy. LTE, EPS & IMS consist of independent functions that are linked by published interfaces. This fosters federation of functions 'horizontally', along the layered network model. This autonomy of network layers allows separate business entities to administer layer-based service, thus avoiding locking into a single vendor.

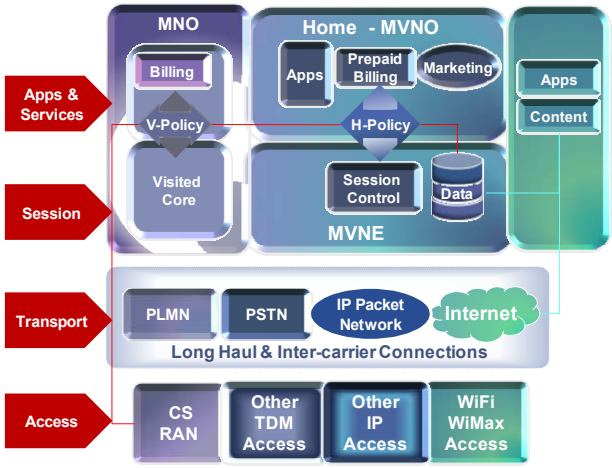

Figure 1: Business Entities in Different Network Layers

In the context of an MVNO, as shown in *Figure 1*, the MVNOs' applications and customer services occupy the top layer. Applications may also come from the MNO and from SPs. If an MVNE (Mobile Virtual Network Enabler) is engaged, it is responsible for the Session Control layer on behalf of the MVNO. The Transport layer is served by the wholesale Telcos (e.g. the MNO), and by IP Trunk providers. The access layer providers are Radio Network Operators, WiFi hotspots, DSL and Cable operators.

The clear definition of interfaces between the network layers allows the MVNO and MVNE models to flourish, but also highlights inherent drawbacks, especially the need to cross business borders in the performance of a single connection. The inter-layer interfaces need to be pre-configured or secure with mutual authentication, tunneling and encryption. Additionally, messages have to travel through more nodes, increasing processing time. However, these issues are mitigated by the EPS efficiency and the flat design that removes a layer of Radio Access nodes.

B. From 'Thin' MVNO to 'Full' MVNO

Initially, MVNOs focus on marketing and the reselling of MNO services, to which end they just need BSS systems ('Thin' MVNO). They often enter the market with a Prepaid Service platform to attract new users. This allows them to compete by setting their own pricing and enforcing usage restrictions and credit control.

To manage subscribers better and distribute their own SIM cards, 'Thin' MVNOs go on to operate their own HLR (Home Location Register), but they also need to associate multiple user identities, for legacy and advanced services, supporting triple/quad play on multiple terminal types. They choose to manage an MSC (Mobile Switching Center) not necessarily to provide full Voice services but to support their IN Camel services and Messaging, and to obtain offline 'post-paid' records of their own.

Many MVNOs attract subscribers through Mobile Broadband services, so they invest in GGSN (Gateway GPRS Service Node). They need to serve 3rd parties content 'remotely' via MNOs' Packet Data Gateways (PDGs) but also collect user intelligence for marketing and advertising purposes, for which they may run their own PDGs. MVNOs also would like to exploit WiFi as free access network resource and may have their own ISP and a Data Network.

Partial or 'hybrid' MVNOs have to integrate into the MNO network. They may be allocated a segment in the MNO's network (MSC+HLR), but this is managed by the MNO who is also a competitor. MVNO may opt for buying some equipment, in which case they are often forced to purchase the same equipment as deployed by the MNO in order to minimize integration effort. By contrast, 'Full' MVNOs (see Ref [14]) have the freedom of selecting their equipment suppliers and the technology level that suits them.

C. MVNO as a 'Home' Network with 'National Roaming'

In roaming scenario, the access is provided by one MNO (the Visited Network) while core functions (authentication, session control and services) are provided by another MNO (the Home network). An MVNO with a full core system can be regarded as the 'Home' network whereas the MNO is always the Visited Network access. This model has the advantage of re-using established roaming procedures and interfaces, therefore requires no special integration effort

than any other roaming partner. This makes it easy for MVNOs to strike deals with multiple MNOs.

For MVNO purpose, the roaming model, which previously only applied to visitors from other countries, had to be adapted for 'National Roaming'. This was pioneered by Hutchinson 3UK in 2003, when the UK regulator (Ref [6]) instructed MNOs to open their networks to new entrants who lacked full coverage. National Roaming has since been adopted in many countries, and can be extended to MVNOs.

Unlike full operators, the MVNO is always a Home network, never a Visited network, so there is no scope for reciprocal roaming agreements. However, the MVNO is a real Home network when the MVNO subscribers roam to other, unrelated networks. When such roaming calls are 'Home Routed', they pass through the MVNO PDGs instead of the MNOs' gateways, bypassing the MNO altogether.

One major difference between MVNO calls and other MNOs' roaming calls is the rate charged by the MNO for connecting MVNO subscribers. Although appearing to be roaming, the MNO has no connection charges, so 'on-net' call charges should apply. Similarly, MNOs cannot charge termination fees for MVNO subscribers, since all incoming calls (except when actually roaming) terminate via the MNO's access. Therefore, MNOs charges are negotiated (and regulated) as a special case, not as normal roaming.

D. *Full MVNO migrating toEPS*

As LTE is rolled out, MVNO with equipment have a new access to connect to. If they already operate MSC or Mobile Softswitch plus a GGSN, they now need to migrate to EPS.

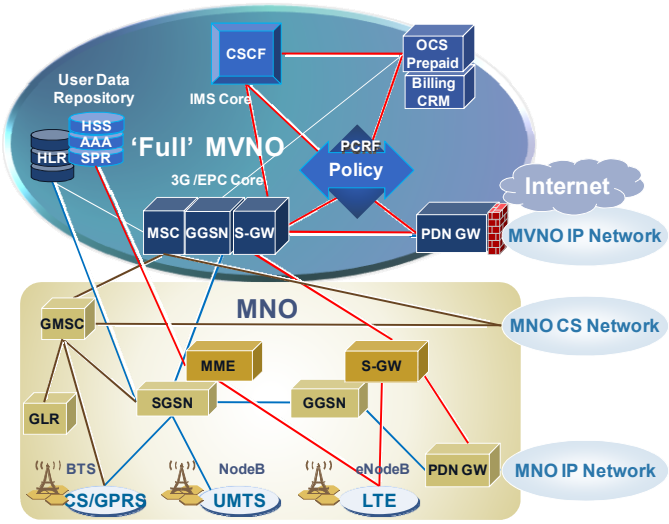

Figure 2: Typical 'Full' MVNO architecture in 3G and 4G

Figure 2 shows the equipment that needs to be in the MVNO core for a Full MVNO model and the evolution of the GPRS to LTE. It also shows the MNO equipment that MNOs deploy in order to accept such roaming traffic. The GMSC (Gateway MSC) and GLR (Gateway Location Register) can interact with partnering MVNOs (see Ref [7]).

MVNO with their own EPS can connect to multiple MNOs, selecting the best option for the user. MVNOs with their own Internet access and packet data gateways can exploit untrusted access networks, without commercial partnering agreements, yet provide carrier grade security.

IV. ENHANCED FEATURES THAT IMPACT MVNOS

A. *Launching Services with VoLTE & IMS (Issue 1)*

The migration to VoLTE entails deployment of IMS, which underpins the ability to launch services independently. MVNOs have an opportunity to expand if they become Full MVNO and introduce IP based Voice on IMS.

MVNOs who have already installed IMS for PSTN replacement are best placed to extend their IMS core and launch Fixed-Mobile convergent services. They can do so even ahead of their MNOs and introduce innovative Voice and non-Voice services on IMS, at their own pace.

B. *MVNO interworking with MNO's Access (Issue 2)*

The Evolving Packet System design changes the roles of the network elements and separates out the core from the access. The EPS Mobility Management Entity (MME) ascertains the location of the mobile device but further session signaling is conducted directly by the S-GW (Serving Gateway). Other GGSN functions are implemented in the S-GW which controls the session and routes traffic to the Internet or to the transport nodes (Ref [5]). This separation of functions enables MVNOs to operate the S-GW, while the MME remains in the MNO network.

MVNO with full core functions look to the MNO as a Home Network for roaming users. The MME retrieves the user's S-GW location from the MVNO's HSS (Home Subscriber Server) and user policies from the MVNO's PCRF (Policy and Charging Rules Function). Session requests and services are served from the Full MVNO's Home network. These are normal roaming procedures that are well established and need no special integration.

C. *Controlling User Data and IDs (Issue 3)*

MVNOs with HLRs can control user provisioning and user location information. For EPS, they can combine HLR and HSS data as well as Policy profiles and AAA for non-3GPP access in a single Data Repository, as defined in Ref [2]. This is important to MVNO who differentiate via triple/quad play and need to provide consistent treatment of the user across multiple terminals and technologies.

Owning User Data allows MVNO to manage users' identities without disclosing sensitive information to the MNO, who may also be a competitor. The standard roaming interfaces ensure that users' location, authentication and QoS/policy profiles can be handled within the MVNO platform (see *Figure 3).*

The MVNO's Online Charging Server remains in control of the user's credit and usage thresholds. It obtains usage information from the Packet Data Gateways. The PDG may be in the MNO's network (*option 1*), or in the MVNO's

network (*option 2)* when using 'Home Routing'. In both options, the MVNOs retain full control of subscribers' sessions, capping, charging rates and policies.

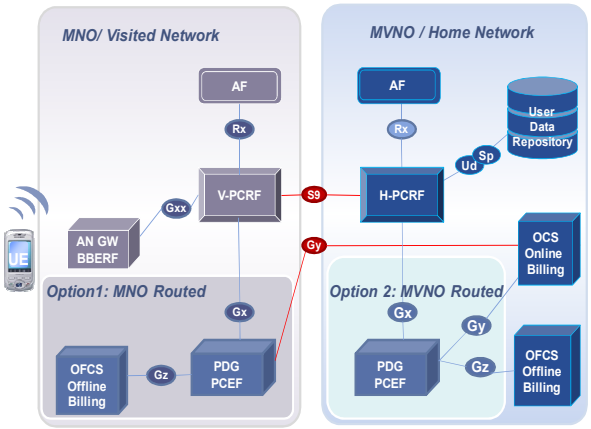

Figure 3: Policy Enforcement across MVNO and MNO domains

D. *Enforcing Policy Rules Remotely (Issue 4)*

Policies were first designed for internal control of resources and charging within a single network. However, end-to-end quality is essential for advanced services, and subscribers' restrictions, conditions and rules must be applied wherever the users' terminals are.

In EPS, the allocation of resources is decided in the Policy and Charging Rules Function (PCRF), as described in Ref [1]. The PCRF is positioned in the core rather than in any access node. The PCRF can then support call admission and installation of policy rules regardless of the type of access. The PCRF scope is extended in 3GPP Release 10 (Ref [3] & [4]) to convey policies between network operators for roaming scenarios. They provide several advantages for an MVNO whose subscribers are always roaming. The MVNO can inter-operate with multiple MNOs and convey policies to them over the standard interface between the Home-PCRF and the Visited-PCRF, as shown in *Figure 3*.

MVNOs define QoS profiles, policies and charging rules for their subscribers, with trigger points and associated actions. The trigger points are conveyed to the MNO's Visited-PCRF, to be installed on the Visited access gateways, to notify the MVNO of any access-based event. Similarly, the MVNO PCRF sends the MNO's PCRF the session parameters to be enforced on the transport gateways, whether they are in the MVNO's own network or elsewhere.

In order to manage users' credit and capping, the Online Charging System (OCS) needs to receive usage reports from the transport gateways. In *Figure 3 option 1,* the MVNO is using the MNO's IP Transport, therefore links the MNO Transport nodes and the MVNO OCS/Prepaid server. This enables more efficient enforcement of capping remotely, across business entities. In *Figure 3 option 2* (MVNO routed), the traffic is diverted via the MVNO's own PDG, which is connected internally to the MVNO's Charging Systems.

E. *Alternative & Untrusted Access (Issue 5)*

Alternative and untrusted access networks provide MVNO access resources free of charge, therefore MVNO, like other network operators, seek to exploit them.

EPS is access agnostic and can serve both trusted access, (with commercial relationships), and untrusted access (unmanaged or unknown). The integrated identity management and user policies enable MVNOs to accept terminal session requests from non-3GPP access (e.g. DSL) as well as LTE. In the case of trusted non-3GPP, for example MNO managed WiFi (managed home gateways or MNO's hotspots), users can be authorized via 3GPP standard AAA servers (see *Figure 4*). MVNOs can agree with MNOs to use a 'Proxy 3GPP AAA Server' to reach their own AAA server, in the same mechanism as for roaming Data users.

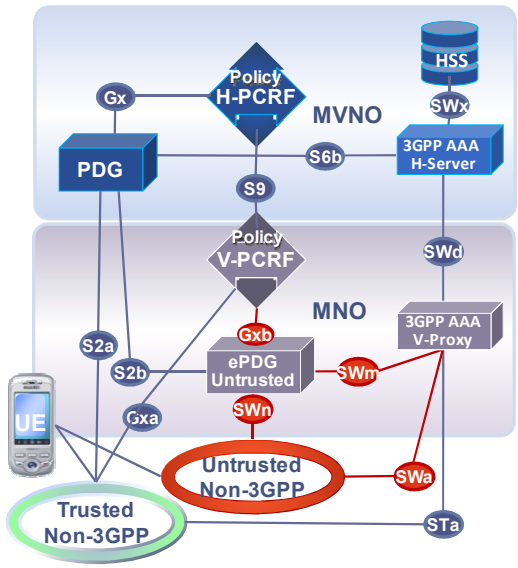

Figure 4: Untrusted non-3GPP Access

There are some additional security requirements for untrusted networks, such as unmanaged WiFi. In the new architecture, the untrusted access traffic is dealt with in the ePDG (Evolving Packet Data Gateway). The ePDG support non-3GPP protocols, such as PMIP (Proxy Mobile IP) and provides further security mechanisms, such as tunneling, that otherwise are not needed.

F. *Detecting User Behaviour and Context (Issue 6)*

To monetize Internet services, MVNOs need to collect subscriber information in real-time and trigger events that may change the session. The sessions need monitoring from both access side and transport network side, recording different events and applying different policies.

EPS separates out the BBERF (Bearer Binding & Event Reporting Function), so that it can be in any access node, LTE or WiFi for example. This enables MVNOs to communicate to any compatible BBERF, whether it is the MNO's own access or not (see *Figure 5*).

User behaviour and usage in the transport network is observed and analyzed by the Traffic Detection Function, also known as Deep Packet Inspection. Traffic Detection is used for shaping traffic to optimize network performance and avoid congestion. It is also used for filtering threats and other security purposes. This function has become even more important because it can collect information on users' Internet activities, preferences and context that are essential for Mobile targeted advertising and context-based services, especially commercial transactions.

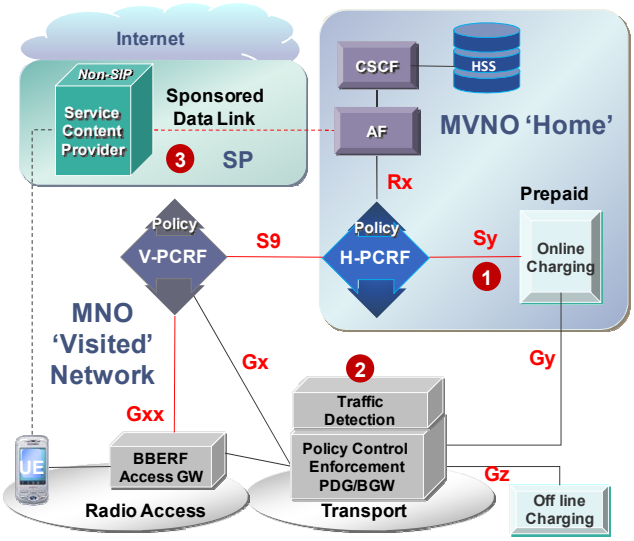

Figure 5: MVNO with 1) PCRF to OCS, 2)Service Traffic Detection Policy 3) Sponsored Data

When MNO divert Internet traffic through WiFi access to reduce 3G congestion, the MVNO GPRS nodes are bypassed and the precious user behaviour information is lost. Operators solve this by forcing such traffic to pass through dedicated traffic monitoring gateways. MVNOs can do the same and force traffic through their own PDG, using the 'Home Routing' option. This can be operated for both trusted and non-trusted traffic, to ensure that the Traffic Detection function on these gateways collects all the desired user intelligence.

Forcing traffic through distant Home gateways may be worthwhile but can be costly. These costs can be mitigated by using Home Routing selectively, to monitor certain high-value users, and ignore other traffic. The selection of users to be monitored can be governed by user-specific routing policies, stored on the H-PCRF and conveyed to the MNO.

G. Variable pricing, credit and quota control (Issue 7)

Value charging instead of a flat rate is essential for MVNO's fine-tuning of margins. MVNOs must match the MNO's charging regime, to avoid charging flat rates to users while paying the MNO for volume usage. Variable pricing can also increase revenues in saturated markets. The tool to achieve that is the Policy Server that installs and varies charging rules for users and for particular services according to context, calendar and location.

The PCRF charging rules can also be used for enforcing quota and credit. MVNOs with Prepaid systems need to control users' calls according to the remaining credit and authorize the MNO to connect or disconnect accordingly. MVNOs also have to comply with the European Directive (Ref [9]) to avoid 'bill shock' for roaming Data users. They must monitor spending (not just volumes) and notify users when charges exceed certain limits. This requires the MVNO's Online Charging System (OCS) to instruct the MNO's gateways to authorize or disconnect sessions.

Current solutions enable the OCS to inform the enforcing network nodes when the spending limits have been reached, (Gy interface, *Figure 5 #2*). However, the new interface between the OCS and the PCRF (see *Figure 5 #2*) enables greater flexibility for MVNOs. This allows for the interaction between the OCS and the Policy Server to occur within the Full MVNO core, and only when action is required will the MVNO PCRF contact the MNO's PCRF and request changes to the charging policies.

H. Connecting to 3rd Party Service Providers (Issue 8)

To monetize content delivery via MNOs, the MVNO acts as an intermediary between the 3rd party content provider and the MNO. Managing these scenarios is particularly important to MVNOs who seek differentiation via Content. The procedure requires passing service authorization information between the Service Provider (SP), via the sponsoring agent (the MVNO) to the carrying network (MNO), where the SP has no commercial relationship with the MNO.

As shown in *Figure 5 #3*, the MVNO/sponsor relays to the MNO's transport nodes information on the authorized duration, QoS levels and termination triggers. The MVNO authorizes the connection to the SP according to the user's profile or the remaining credit in the user's account. Policies and events (such as exceeding the authorized amount/duration/volume) are communicated between the networks via the respective PCRFs and, if needed, passed also to the Online Charging Server.

I. Access Network Discovery & Selection (Issue 9)

When the terminal seeks to make a connection, it may have a choice of several local networks as well as access providers. The choice is governed by the terminal technologies and capabilities and by existing agreements with access providers.

The standards define an Access Network Discovery and Selection Function (ANDSF), to recognize and negotiate with available access networks and apply policies by which operators can assist (but not dictate) the selection. The ANDSF function can exist in the Home network (MVNO) or the Visited network (MNO) or both. It conveys to the terminal rules for selecting an access network, with prioritized partner lists, local restrictions (e.g. roaming data rules) and preferences (e.g. WiMax is preferred to WLAN). In the case of MVNOs, ANDSF allows them to apply their priorities for access modes and partners on behalf of their subscribers, whether they are within the MNO's space or truly roaming. Therefore, this facility is an important enabler

of 'Always Best Connected', where the MVNO help to select the best choice of access.

J. Secure Attachment to Access Network (Issue 10)

Connection to unknown and unmanaged access networks brings further risks that both MNOs and MVNOs must tackle. EPS provides higher security mechanism using AKA (Authentication and Key Agreement) and EAP (Extensible Authentication Protocol). They can be used during the process of attaching to an access network too, and add security to the ANDSF process.

Additional security is provided via the ePDG, as shown in *Figure 4* above. The ePDG is a special packet data gateway for untrusted services. It supports protocols that are used by such traffic, e.g. PMIPv6 (Proxy Mobile IPv6). The ePDG forms security association with the handset for tunneling through the untrusted network and provides encryption/decryption facilities for the service data flows.

V. SUMMARY

In this paper, remedies for ten persistent MVNO issues have been identified. The EPS architecture enhances MVNO independence from the MNO network. The 'Full' MVNO can use the standard roaming scenarios, which provide established interfaces and well tried procedures.

Several important features have been introduced to EPS for roaming that help solving MVNO worst issues. This includes the H-PCRF to V-PCRF interface, the PCRF-OCS and the PCRF to BBERF links. They enable MVNOs to convey their own policies dynamically across to the MNO's network elements. They support triggering events in the MNOs' networks, and monitoring thresholds and charging events in the MVNO core. These features also enable value pricing and fine-tuning of margins by connection to the Online Charging System.

Full MVNOs gain not only independence, but also the ability to connect to several access networks, trusted and untrusted. They can utilize smart access selection through the access discovery and selection method, to optimize network costs and exploit the free WiFi resources. They can also utilize Home Routing to divert service data flow through their own gateways, and obtain user intelligence from their own Traffic Detection facilities.

The following table provides the list of ten persistent MVNO issues and their remedies via new methods and standard interfaces.

No	Key Issues Description	Remedy Solution
1	Ability to introduce services independently	'Full MVNO' with IMS for VoLTE can introduce services independently of MNOs
2	Interworking & inter-administration interfaces	With MVNO EPS, the interfaces are clear and standard-based. MVNOs can connect to multiple MNOs, using established roaming users procedures
3	Controlling user IDs for Tripple play without disclosing user information to MNO	Unified user data allows linking identities while keeping credit information within the MVNO data
4	Enforcing Policy through another network/access	Visited-PCRF to Home-PCRF links allow conveying policy remotely, to be enforced by other MNO networks
5	Supporting alternative and untrusted access networks	EPS access-agnostic nature, unified Data (with AAA and SPR) and ePDG support multi-terminal users, with non-3GPP and untrusted access networks too.
6	Detecting user behaviour and context Data	Home Routing with Deep Packet Inspection enables MVNO to retain knowledge of user behaviour
7	Variable pricing, credit and quota control	The ability to convey charging rules across networks (S9) and connect to OCS directly allow MVNO to provide variable charging and apply charging caps etc.
8	Connecting SP service through another network and get paid	Sponsored Data interfaces transfer identities of 3rd parties via intermediaries, allowing charging information exchange and capping to be applied
9	Selecting best alternative access network	ANDSF provides means of establishing available access connection with prioritized access networks
10	Securing Internet and untrusted access	The ePDG can support untrusted access networks with carrier grade security

REFERENCES

[1] 3GPP TS 23.203 Policy and Charging Architecture Rel 11

[2] 3GPP TS 23.813 Study on Policy solutions and Enhancements

[3] 3GPP TS 23.402 Architecture Enhancements for non-3GPP accesses Rel10

[4] 3GPP TS 23.401 GPRS enhancements for eUTRAN Release 10

[5] J J Pastor Balbas, Stefan Rommer & John Stenfelt, "Policy and Charging Control in the evolved Packet System", IEEE Communications Magazine, Volume 47 Issue 2, February 2009

[6] Oftel UK, National roaming condition, A consultation on proposals to set a national roaming condition after 25 July 2003

[7] 3GPP TS 23.002 Network Architecture Release 10

[8] Wikipedia Mobile virtual network operator

[9] European Parliament and the Council, "Regulation (EC) No 544/2009 of the European Parliament and the Council 18 June 2009 amending Regulation (EC) No 717/2007 on roaming on public mobile telephone networks"

[10] Rory Graham, MVNOs, Key Legal Issues, Coffey Graham LLP 2010

[11] T. Bassayiannis, "Mobile Virtual Network Operator (MVNO)", Athens Information Technology MBIT Thesis, December 2008

[12] Santi Pattanavichai et al, "A Pricing Model and Sensitivity Analysis for MVNO Investment Decision Making in 3G UMTS Networks", IEEE Symposium 2010, Penang, Malaysia

[13] Abdul Hameed Al-Sunaid, i2 Group, SAMENA Telecommunications Council, "Beyond Connectivity", January 2007, Dubai –UAEP

[14] Rebecca Copeland, Noel Crespi " Modelling Multi-MNO Solutions for MVNOs and their Evolution to LTE, VoLTE & advanced Policy"