Multi-vendor Auto-Connectivity in Heterogeneous Networks

Péter Szilágyi
Nokia Siemens Networks Research
Budapest, Hungary
peter.1.szilagyi@nsn.com

Henning Sanneck
Nokia Siemens Networks Research
Munich, Germany
henning.sanneck@nsn.com

***Abstract*—Heterogeneous radio networks (HetNet) consist of base stations and other Network Elements (NE) manufactured by various vendors, providing service at overlapping coverage areas supporting different Radio Access Technologies (RAT). This heterogeneity increases the complexity of network management functions as the required infrastructure, configuration sequences and protocols vary across vendors. The diversity also makes the automation of initial configuration (referred to as self-configuration or "plug-and-play") an essential element in providing easier and faster network roll-out and base station deployment, especially considering emerging RATs such as Long Term Evolution (LTE) and beyond. Therefore, the need for a simple, unified auto-connectivity has become increasingly important with the evolution of 3G and LTE deployments towards HetNet infrastructures. In this paper, a novel multi-vendor capable self-configuration architecture is presented, which was inspired by real network deployment and auto-configuration scenarios. The proposed framework is able to provide a unified initial connectivity sequence for new network elements including base stations supporting different RATs. Additionally, the proposed apparatus is also prepared for handling multiple Domain Manager (DM) instances under the supervision of the same vendor and within the same RAT. The standardization impacts of the proposed architecture and the required technologies are discussed as well.**

Keywords*—*Auto-connectivity; multi-vendor; plug-and-play; self-configuration

I. Introduction

Heterogeneous networks are becoming common nowadays at an increasing number of mobile network operators, both in current deployments and future network evolution plans in order to provide enhanced capacity at hotspots and urban areas as well as better indoor coverage. The term HetNet refers to both multiple resource (cell) layers within the same radio access technology as well as the coexistence of different RATs; a common example for the former is given by the differently sized LTE cells where macro cells provide coverage at a larger granularity and micro, pico and femto cells are used to provide concentrated services and availability. The gradual deployment of newer generation radio access technology, such as LTE, next to already deployed Wideband Code Division Multiple Access (WCDMA), High Speed Packet Access (HSPA) and Global System for Mobile Communications (GSM) cells results in coexisting technology layers.

In HetNet scenarios, network operators deploy a large number of NEs, mostly base stations such as WCDMA Node Bs, LTE evolved Node Bs (eNB) and LTE micro, pico or femto cells. Multi-mode base stations supporting multiple RATs within one cabinet and shared antenna system are also commonly available. The equipments providing different resource layers (both intra-RAT and inter-RAT) are often purchased from different vendors. Also, to decrease the risk of vendor lock-in, some operators tend to obtain and roll out base stations from at least two different vendors even for providing services over the same RAT. At the same time, considering the complexity introduced by the coexisting layers, multiple vendors and the sheer number of the NEs, the deployment of new NEs is required to be plug-and-play, i.e., no pre-configuration should be required in the factory prior to field installation and no (or as little as possible) local on-site configuration should be performed during field installation. However, currently different vendors employ different auto-connectivity sequences and require different protocols and supporting nodes such as Dynamic Host Configuration Protocol (DHCP) servers and may also have particular requirements on the Virtual Local Access Network (VLAN) and Internet Protocol (IP) domain layout for their solution to work. This raises difficulties for the network operator because the different plug-and-play methods of the various vendors eventually need to be integrated into a common solution by multi-vendor integration. In practice, the first vendor deploys its plug-and-play infrastructure and forthcoming vendors have to adjust their auto-connectivity and plug-and-play sequences to that of the first vendor. Of course, a particular vendor being the first one in an operator's network may be at the same time the second one in another network, which means that multi-vendor plug-and-play integration not only comes with additional cost and delayed deployment for the network operators but raises difficulties and overhead for vendors as well. Additionally, there is not much possibility for vendor differentiation in auto-connectivity anyway as this is not a service that impacts the user experience of the mobile subscribers or the quality of service a network is able to provide during the operation stage.

The first step of the configuration of a network element is the establishment of the initial connectivity between the NE and the Operation, Administration and Maintenance (OAM) system of the network [1]. This step is the most diverse considering the wide range of various vendor specific implementations; therefore, a unified solution for this step, similarly to the one that has already been standardized for LTE-Advanced Relay nodes [2], would significantly reduce the overhead of multi-vendor integration as well as the latency of network roll-out and the time to market of new services requiring network expansion.

The initial connectivity of a network element is used for transferring configuration data from the OAM system to the network element. In case of base stations, the configuration data is not created for a particular network element but for the site where a base station is to be installed. When a specific base station hardware is deployed at a site, it is the responsibility of a hardware to site mapping process [3] to identify the physical site (e.g., building, rooftop, mobile tower, etc.) at which a given NE instance is installed and, based on that site identity, the corresponding site configuration data is conveyed from the planning database to the NE during the auto-commissioning process.

In this paper, a multi-vendor auto-connectivity solution for 3G/LTE networks is presented based on experience from real network deployments, which can harmonize the initial connectivity sequence of NEs from various vendors in a HetNet environment. The mechanism provides an initial auto-connectivity sequence that connects the NEs from various vendors and RATs to the DM node in the OAM system that contains the corresponding configuration data. The multi-vendor requirement basically means that at some point in the auto-connectivity sequence the vendor identity of the NE has to be mapped to specific network nodes; the implementation of the mapping is realized by utilizing features of well-known and commonly used protocols such as the DHCP or Domain Name System (DNS).

The rest of this paper is organized as follows. In Section II, the detailed requirements of a multi-vendor solution are discussed. Section III presents the proposed multi-vendor plug-and-play architecture, the required infrastructure including nodes and protocols as well as the initial connectivity sequence of new NEs from the beginning until they are securely connected to the corresponding DM node. The standardization impacts and status of the solution are also discussed. Finally, Section IV concludes the paper.

II. Requirements of Auto-Connectivity

The key requirements for the self-configuration of NEs (particularly base stations) in heterogeneous environments can be summarized as follows; some of these are synthesized by the Next Generation Mobile Networks (NGMN) Alliance [4] and others are reported by operators [5]:

1) *Multi-vendor:* The NEs manufactured by various vendors should be able to connect to the DM nodes in the OAM system of the network in a uniform (possibly standardized) way, without requiring pre-configuration of any vendor specific data in the NEs prior to field installation (facilitating multi-vendor plug-and-play deployment).

2) *Multi-RAT:* This requirement applies specifically to base stations and not generally to any type of network elements. Base stations supporting a particular RAT are usually configured by a DM node in the OAM system that is different from those used for other RATs; therefore, it is not enough to connect a base station to the corresponding vendor's DM in general but also to the node being responsible for its RAT. Although there is an increasing trend for multi-radio base stations among various vendors, in which case a base station implements multiple RATs (e.g., GSM, WCDMA and LTE), the configuration of the different RATs may still be done by separate DM nodes in the OAM system; nevertheless, a self-configuration solution should be able to automatically connect a new NE to the right DM node of the corresponding vendor.

3) *Multi-DM:* Besides multi-RAT requirement, multiple DM nodes corresponding to the same vendor and even to the same RAT (e.g., multiple vendor "A" LTE DM nodes) should be supported. The rationale behind this requirement is that for various reasons (such as load balancing), the site planning and configuration data may be distributed among several DM nodes even for the same RAT and vendor and there is a one-to-one mapping between a site and the corresponding DM node. Thus, the plug-and-play solution should not simply connect a new NE deployed at a specific site to an arbitrary DM with matching vendor and RAT but also to the particular DM node that hosts the site configuration data.

Additionally, operators have defined general requirements for advanced plug-and-play solutions, which need to be addressed to enable widespread adoption. A general requirement is VLAN/IP domain separation, which means that the operator's VLAN and IP access network should be split into two parts: a *plug-and-play* (PnP) access domain and an *operational* (OPE) access domain. The PnP domain, accessed by NEs for the first time, is shared by all vendors that have deployed or are going to deploy NEs in the operator's network. Given the more open (and, consequently, less trusted) nature of the PnP domain, only basic configuration of the NEs should be performed through that, mostly resorting to providing the NE with enough information that enables it to connect to the right DM node via the trusted and secure OPE domain.

Security of the initial connectivity is another important aspect; a strict security requirement is that multi-homing in both access domains (i.e., a node with interfaces in both PnP and OPE domain) is to be avoided. Since nodes directly accessible from the PnP domain may be considered as less secure, i.e., more exposed to attackers, their separation (by firewalls, for example) from nodes residing in the trusted OPE domain is desired. Nevertheless, even with such separation in place, it is still recommended to resort to security mechanisms, e.g., Transport Layer Security (TLS) and (optionally) Internet Protocol Security (IPsec) between NEs and network nodes within the PnP domain to prevent eavesdropping and tampering as well as to implement mutual authentication.

The practical choice of network protocols based on which the plug-and-play connectivity is implemented is also important. A particular problem that should be taken into account has been identified by difficulties encountered during real network roll-out and it is related to the usage of the DHCP protocol [6] for vendor differentiation. In order to provide information to the NE about how to access the DM that is specific to its vendor, DHCP options would have to be used: the Vendor Class Identifier (DHCP option 60) and the Vendor Specific Information (DHCP option 43) for requesting and retrieving vendor specific information [7]. However, these DHCP options are not well or consistently supported by existing open source and commercial DHCP implementations such as DHCP servers integrated in network devices like routers. Also, even if the required options are implemented, the provided capabilities may not be sufficient to realize the use case (e.g., DHCP options

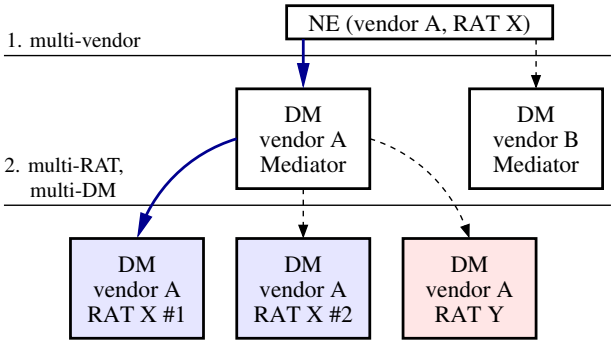

Fig. 1. Illustration of the multi-vendor and multi-RAT/-DM functions of the proposed auto-connectivity framework.

longer than 255 characters are not supported). Therefore, it is difficult, if not impossible to implement the multi-vendor requirement based on DHCP alone.

Until now, no common solution has been provided and agreed on by operators, vendors or standardization bodies. While the 3rd Generation Partnership Project (3GPP) Service and System Aspects (SA) Working Group 5 (WG5) has standardized an "Itf-P2P" as a multi-DM "east-west-bound" interface [8], Itf-P2P has not found practical acceptance. The standardization of additional DHCP options would not be practical either due to the limitations of the DHCP itself as discussed above. Therefore, in order to fill this gap, a multi-vendor, multi-RAT and multi-DM plug-and-play architecture is proposed in this paper, which is capable of meeting all the above requirements while keeping implementation cost down on both vendor and operator sides.

III. Multi-vendor Plug-and-Play Architecture

In the proposed multi-vendor, multi-RAT and multi-DM capable framework, the auto-connectivity of a new network element consists of two stages. First, the vendor identity of the NE is resolved and the NE is connected to a novel entity referred to as the *Mediator DM*, which is capable of processing and interpreting vendor-specific messages. Second, with the assistance of the Mediator DM, the NE is connected to the specific DM node storing the detailed configuration data that needs to be conveyed to the NE prior to its operational phase. These two stages are also referred to as the first and second level of indirection, respectively. The first stage implements multi-vendor capability and the second provides multi-RAT and multi-DM capabilities. There is one Mediator DM for each vendor in an operator's network, with the task of implementing the multi-RAT and multi-DM capabilities. The overview of the architecture is shown in Fig. 1.

In order to avoid the DHCP issues known from field experience, the proposed architecture decreases the role of DHCP in favor of using the DNS [9], [10] in order to differentiate between vendors, i.e., it uses DNS instead of DHCP to connect new NEs (mostly base stations) to the DM of their respective vendor. The next subsection provides an overview of the entities (nodes, protocols) that are employed in the architecture and their roles in the multi-vendor plug-and-play process.

A. Supporting entities

Apart from the NE to be configured, the supporting apparatus consists of the following nodes:

DHCP server: The role of the DHCP server is limited to the allocation of a temporary PnP domain IP address for the connecting NE and signaling the IP address of the DNS server. These are standard functionalities supported by all DHCP implementations; therefore, the dependency on the unsupported vendor specific DHCP extensions is eliminated.

DNS server: Used to resolve operator specific and vendor specific domain names (detailed later) and it returns the IP address of the operator's Certificate Authority (CA) server as well as the IP address of the corresponding vendor's Mediator DM, thereby implementing the multi-vendor requirement.

Mediator DM: There is one such dedicated node for each vendor in an operator's network, accessible from the PnP domain. It stores initial configuration data of all sites of the respective vendor but has no detailed planning data. The initial configuration data is limited to the information needed for NEs to connect to the OPE access domain, including the final OPE IP address of the NE itself and the OPE IP address of the DM node containing the corresponding detailed planning data.

Other DM nodes: Contain the detailed planning of sites. Unlike the above nodes, which are accessible from the PnP domain, these nodes can only be accessed from the trusted OPE domain.

CA server: It provides Public Key Infrastructure (PKI) information to be used for secure connectivity between the NE and the Mediator DM in the PnP domain. There is one such entity in an operator's network and all equipments from all vendors use that to obtain PKI information.

The proposed solution uses DNS to provide the first level of indirection, implementing the multi-vendor requirement. The usage of DNS facilitates deployment as only a single server in a network domain needs to be maintained and there are no known problems of interoperability between DNS protocol entities (as opposed to the potential practical issues of using DHCP for that purpose). Some IP router vendors offer built-in DHCP and (or) DNS server services in their product. If the network operator uses such routers, the proposed solution can be implemented without the need for physically deploying new nodes for providing the necessary DHCP and (or) DNS functionalities, thereby mitigating the deployment and maintenance cost of these services.

The Mediator DM nodes are introduced to provide the second level of indirection, implementing the multi-RAT and multi-DM requirements. Each vendor's Mediator DM is a frontend to the vendor's other DM nodes: the Mediator is the entity that is first contacted by new NEs; it maps the NE to one of the other DM nodes that contains the detailed planning data of the site to which the NE has been deployed; it provides the NE with the initial connectivity information that enables it to connect to the DM node via the OPE access domain. The mapping of a new NE to the appropriate DM node can

be vendor specific, e.g., based on the NE's type, capabilities, supported RATs.

When a network expansion is planned, possible deployment sites for a given vendor's base stations are identified. For each site, a detailed site plan is created with the operator's planning tool and the planning data is uploaded to one of the vendor's DM nodes. This DM node then has to upload the initial configuration part of the planning data to the respective vendor's Mediator DM. The initial configuration data is a subset of the detailed planning data and it contains at least the following entries: (a) NE OPE VLAN ID; (b) NE OPE IP address; (c) default gateway IP address; (d) DM OPE IP address; and finally (e) the IP address of the Security Gateway used to separate the trusted OPE domain from other network parts (in case IPsec is used in the connection between the NE and the Mediator DM).

According to operator specific requirements, the interface between a vendor's DM nodes and its Mediator DM may be unidirectional, which means that connection establishment is only possible from one of the DM nodes towards the Mediator DM (for uploading the initial configuration data) but not vice versa; this can be implemented, e.g., by a firewall. The reason for this design is improved security: if the Mediator DM node is attacked from the PnP domain, there is still no further possibility to compromise any of the DM nodes, preserving the functionality of the OAM system for already established network elements and ensuring the continuity of the auto-configuration service.

B. Naming system

In order to use DNS for implementing the multi-vendor requirement, the nodes involved in the process need to be given fully qualified domain names (FQDN). An operator specific FQDN is proposed to identify the operator's CA server and a vendor specific FQDN is proposed for each vendor to identify its Mediator DM node. The structure of the operator specific FQDN used for the CA server is proposed to be as follows:

```
caserver.mediator
.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

The structure of the vendor specific FQDNs used for the Mediator DMs is proposed to be as follows:

```
vendor<VID>.mediator
.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

where MNC and MCC are the operator's Mobile Network Code and Mobile Country Code, respectively, and VID is a unique Vendor Identifier. These FQDNs are constructed according to the standardized usage of the `3gppnetwork.org` domain [11], which includes several subdomains for different nodes in an LTE Evolved Packet Core (EPC) network. In the above FQDNs, the first line is the extension proposed in this paper and the second line denotes the already standardized part.

As mentioned in the introduction, a requirement for a plug-and-play solution is to avoid any pre-configuration of the NE prior to its deployment as much as possible. Therefore, a solution is required to automatically provision the MNC and MCC of the operator into the NE for constructing the FQDN. Two possible approaches may be used to avoid manual configuration. First, the fixed part of the domain name (i.e., `oam.mnc<MCN>.mcc<MCC>.3gppnetwork.org`) can be provisioned in the DNS server as the system's default domain name; then, the NEs may only send the "`caserver.mediator`" and "`vendor<VID>.mediator`" parts in the DNS query messages and they will be completed by the DNS server with the default domain name to create the FQDN. This can be used in a single operator infrastructure (i.e., when resources such as access/transport network, DNS server, etc. are not shared between different operators) in a straightforward manner. In a shared infrastructure environment, one operator has to take the lead and provide the infrastructure including the DNS server and it is the lead operator's MNC and MCC that is provisioned in the DNS server as the default suffix. As a second alternative, the fixed part of the FQDN can be configured in the DHCP server so that it is sent in the DHCP Ack as Option 15 "Domain Name" [7]. The disadvantage of this approach in comparison with the previous one is that additional DHCP management is required as the default suffix of the domain needs to be configured in the DHCP server. Note, however, that this additional DHCP configuration is still significantly easier than the provisioning of vendor specific DHCP attributes and, contrary to them, it is supported by DHCP implementations.

The operation of the self-configuration infrastructure requires that the IP address of the DNS server resolving the operator and vendor specific domain names are configured in the DHCP server. Unless the DNS server has a dynamic IP, which is almost never the case in real network deployments (and not recommended), this has to be done only once, when the plug-and-play infrastructure itself if deployed. For each vendor's Mediator DM, a specific FQDN is provisioned in the DNS server and kept up-to-date either manually or by the respective Mediator DM via Dynamic DNS [12]. Again, if the Mediators have static IP allocation, the DNS records have to be created only once. Additionally, the IP address of the operator's CA server also needs to be provisioned in the DNS server under the operator specific FQDN.

C. Initial connectivity sequence

The connection sequence is illustrated in Fig. 2 and Fig. 3; the former depicts nodes from a single vendor "A" in order to highlight the multi-RAT and multi-DM capabilities while the latter shows two vendors, "A" and "B", to highlight the multi-vendor capability. For the sake of simplicity, security setup is omitted from both descriptions and it will be discussed separately in Section III-D.

First, the NE may need to run VLAN probing to find the PnP VLAN; then, the NE requests an IP address from the PnP IP domain via DHCP, which also provides it with the IP address of the DNS server. Then, the NE sends a DNS query to resolve the specific FQDN, thereby obtaining the PnP domain IP address of the Mediator DM. At this point, the site identity needs to be obtained by the NE so that it can request the corresponding configuration data. In case the NE is equipped with a Global Positioning System

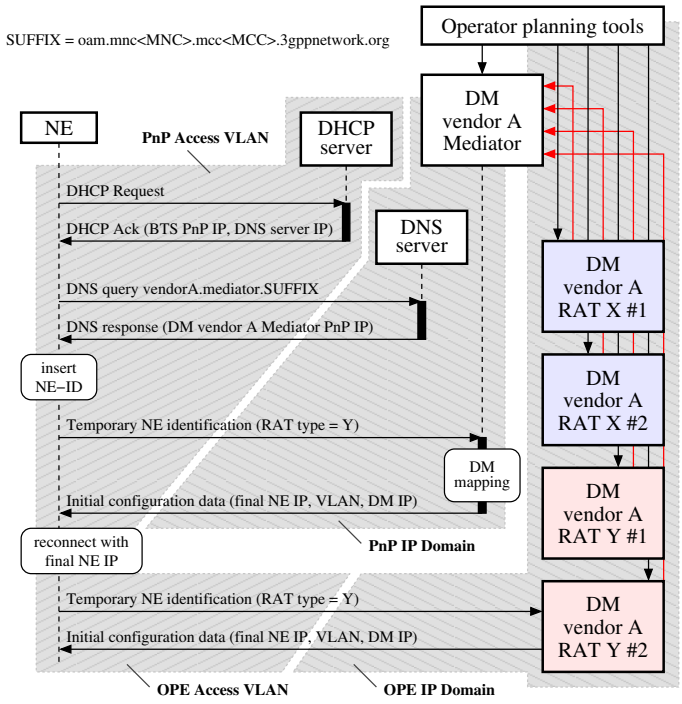

Fig. 2. Initial connectivity sequence, showing the infrastructure corresponding to one vendor.

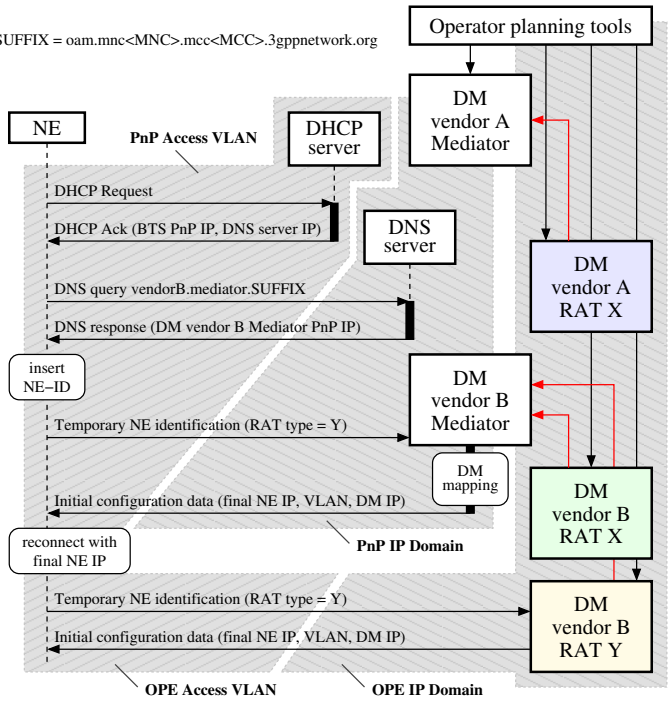

Fig. 3. Initial connectivity sequence, showing the infrastructure of two vendors co-existing in a multi-vendor deployment.

(GPS) receiver, as some base stations are, the coordinates can serve to obtain the identity of the deployment site in a fully automated way. Otherwise, the plug-and-play sequence needs to be interrupted and the field installer should inject an identifier, which is unambiguously linked to the site, e.g., by means of barcode or radio frequency identification (RFID). The NE connects to the Mediator DM and sends the site identifier obtained above; additional information such as the supported RATs or further capabilities can also be sent. Based on the received information, the Mediator DM selects the DM node that contains the detailed site planning data and sends the initial configuration data to the NE to enable its connection to the DM node via the OPE domain. Consequently, the NE disconnects from the Mediator DM and reconnects to the DM via the OPE domain to download the final and detailed configuration, software update, etc., which is required in order for the NE to enter operational phase with the correct configuration.

D. Security setup

In the previous description, the communication between the NE and the Mediator DM was neither authenticated nor encrypted. However, according to operator requirements, it is recommended that security measures are taken already in the PnP domain to avoid the connection of unauthorized or malicious devices to the Mediator DM. Therefore, the NE resolves not only the vendor specific FQDN but the operator specific FQDN as well to obtain the PnP IP address of the CA server, as illustrated in Fig. 4. Before connecting to the Mediator DM, the NE connects to the CA server for the acquisition of PKI information.

In practice, accessing the CA server requires not only the PnP IP address of the CA server but also a port number and optionally a Uniform Resource Locator (URL) as well. The port number is usually set to 829, i.e., the well-known port for the Certificate Management Protocol (CMP) [13]. The URL is the so-called Subject-name of the CA server, which is used to address a logical CA in case the security server hosts multiple virtual CAs; it can be omitted if virtual CAs are not used. Therefore, besides the PnP IP address of the CA server, the port and (possibly) the URL also have to be known to the NE, which can be provided in two ways:

1) Using standardized values (recommended): since there is already a well-known port for CMP, it could be standardized for the plug-and-play infrastructure. Also, the usage of virtual CAs should either be prohibited in the plug-and-play infrastructure or the URL should be a fixed (standardized) one, e.g., "/pkixcmp/3gppnetwork/pnp".

2) Using DNS Text (TXT) Resource Records (RR), there can be a TXT RR associated with the IPv4 (A) or IPv6 (AAAA) RRs containing the CA server's IP address in the DNS server, specifying all required additional information, i.e., the CMP port and Subject-name; in this case, the structure of the TXT RR needs to be standardized, e.g., "port=⟨PORT⟩, path=⟨PATH⟩, subject=⟨SUBJECT⟩".

After the PKI information has been acquired from the operator's CA server, the NE can continue with the connection to the Mediator DM by establishing TLS and optionally IPsec connections, which provides both authentication and encryption. In case IPsec is used, the presence of a Security Gateway is also required.

E. Standardization Impacts

The proposed multi-vendor solution has two standardization impacts: one is associated with the FQDNs required for

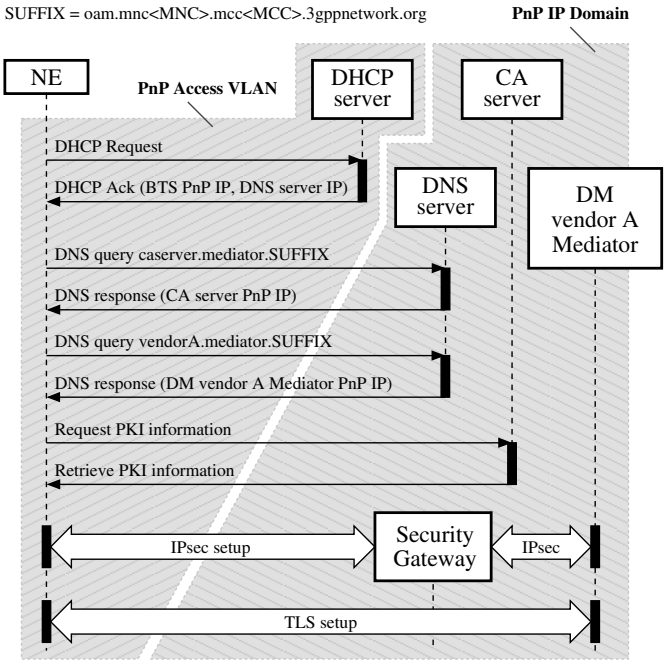

Fig. 4. Secure connectivity setup between the NE and the Mediator by means of TLS for mutual authentication and encryption and optionally by additional IPsec (through a Security Gateway) as well.

the identification of the operator's CA server and the vendors' Mediator DMs; the other is concerning the access of the CA server.

The FQDN structures need to be standardized by the GSMA as specified in Annex E of [11]. Apart from the structure of the FQDNs, the allocation of the unique VIDs is also mandatory for the process to work. The access of the CA server also needs to be standardized; the best alternative with the lowest implementation impact would be to nominate the already de-facto standard well-known port 829 as the standard port for the CMP and either prohibit the usage of the virtual CA service or standardize a URL for the plug-and-play service. This standardization step could also be managed by the 3GPP without having to involve other standardization processes as it should only cover the usage of these parameters in the context of self-configuration in 3GPP networks.

A 3GPP work item aiming at the standardization of the multi-vendor plug-and-play ecosystem presented in this paper has already been started and it is currently in progress [14], supported by leading vendors and network operators.

IV. Conclusion

In this paper, a multi-vendor, multi-RAT and multi-DM capable auto-connectivity solution has been proposed to implement the initial, crucial part of the self-configuration process and harmonize the initial connectivity sequence of NEs manufactured by various vendors. The main characteristics of the solution are the usage of DNS to provide the first level of indirection to implement the multi-vendor requirement and the novel per-vendor Mediator DM nodes to provide the second level of indirection, implementing the multi-RAT and multi-DM requirements. The solution features VLAN/IP access domain separation between the PnP and OPE domains. Authenticated and encrypted communication with the OAM system is assured even in the initial PnP domain. The advantage of the solution is the lowered integration cost for operators; vendors also benefit form a uniform implementation, thereby avoiding most of the integration costs. The standardization of the framework by 3GPP is already in progress.

References

[1] S. Hämäläinen, H. Sanneck, and C. Sartori, Eds., *LTE Self-Organising Networks (SON): Network Management Automation for Operational Efficiency*. John Wiley & Sons, 2011.

[2] P. Szilágyi and H. Sanneck, "LTE relay node self-configuration," in *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, May 2011, pp. 841–855.

[3] T. Bandh and H. Sanneck, "Automatic site identification and hardware-to-site-mapping for base station self-configuration," in *IEEE International Workshop on Self-Organizing Networks, Budapest, Hungary*, May 2011, pp. 1–5.

[4] NGMN Alliance, "Top P-OPE Recommendations," Sep. 2010. [Online]. Available: http://www.ngmn.org/uploads/media/NGMN_Top_OPE_Recommendations_1.0.pdf

[5] Deutsche Telekom, "Full multi-vendor Plug and Play," 3GPP TSG SA WG5 (Telecom Management) Meeting #81, S5-120225, Feb. 2012.

[6] R. Droms, "Dynamic Host Configuration Protocol," RFC 2131 (Draft Standard), Internet Engineering Task Force, Mar. 1997.

[7] S. Alexander and R. Droms, "DHCP Options and BOOTP Vendor Extensions," RFC 2132 (Draft Standard), Internet Engineering Task Force, Mar. 1997.

[8] 3GPP, "Telecommunication management; Application guide for use of Integration Reference Points (IRPs) on peer-to-peer (p2p) interface," 3rd Generation Partnership Project (3GPP), TR 32.806, Jun. 2007.

[9] P. Mockapetris, "Domain names - concepts and facilities," RFC 1034 (Standard), Internet Engineering Task Force, Nov. 1987.

[10] P. Mockapetris, "Domain names - implementation and specification," RFC 1035 (Standard), Internet Engineering Task Force, Nov. 1987.

[11] 3GPP, "Numbering, addressing and identification," 3rd Generation Partnership Project (3GPP), TS 23.003, Dec. 2011.

[12] B. Wellington, "Secure Domain Name System (DNS) Dynamic Update," RFC 3007 (Proposed Standard), Internet Engineering Task Force, Nov. 2000.

[13] C. Adams, S. Farrell, T. Kause, and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)," RFC 4210 (Proposed Standard), Internet Engineering Task Force, Sep. 2005.

[14] Deutsche Telekom, "Multi-vendor plug and play," 3GPP TSG SA WG5 (Telecom Management) Meeting #82, S5-120799, Mar. 2012.