ETSI TS 128 316 V17.0.0 (2022-05)

5G;
Management and orchestration;
Plug and Connect;
Data formats
(3GPP TS 28.316 version 17.0.0 Release 17)

Reference
DTS/TSGS-0528316vh00

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

The present document is part of a TS family covering the 3rd Generation Partnership Project Technical Specification Group Services and System Aspects, Management and orchestration; as identified below:

TS 28.314: "Plug and Connect; Concepts and requirements".

TS 28.315: "Plug and Connect; Procedure flows".

TS 28.316: "Plug and Connect; Data formats".

1 Scope

The present document specifies data formats for *Plug and Connect* NE in 3GPP systems.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 28.314: " Management and orchestration; Plug and Connect; Concepts and requirements".

[3] 3GPP TS 28.315: "Management and orchestration; Plug and Connect; Procedure flows".

[4] IETF RFC 3925: "Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[5] IETF RFC 8415: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[6] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".

[7] IANA: "Private Enterprise Numbers", http://www.iana.org/assignments/enterprise-numbers.

[8] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[9] IETF RFC 3396: "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)".

[10] IETF RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[11] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[12] IETF RFC 6712: "Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)".

[13] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[14] 3GPP TS 23.003: "Numbering, addressing and identification".

[15] IETF RFC 1035: "Domain Names - Implementation and Specification".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1], TS 28.314 [2] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1] and in TS 28.314 [2].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], TS 28.314 [2] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1] and TS 28.314 [2].

4 Data formats for Plug and Connect

4.1 Client identification in DHCP requests

4.1.1 DHCPv4

This clause describes DHCP options for use with DHCP for IPv4 (DHCPv4) that NE uses to identify itself in DHCP requests in Plug and Connect (PnC).

The NE performing the Initial IP Autoconfiguration procedure specified in clause 5.2 of 3GPP TS 28.315 [3], using IPv4 based network stack, may identify itself using Vendor Class Identifier DHCPv4 option 60 as specified in RFC 2132 [6]. The format of Vendor Class identifier shall follow the rules specified in clause 9.13 of RFC 2132 [6], which is illustrated in table 4.1.1.1:

Table 4.1.1.1: Format of Vendor Class Identifier

Code	Length	Vendor Class Identifier		
60	n	i1	i2	…
octet	octet	octet	octet	octet

The NE may identify itself as Multi-Vendor Plug and Connect (MvPnC) compatible DHCPv4 client using DHCPv4 option 60 in the following way:

- DHCPv4 option code 60;
- Length 5 bytes;
- Vendor class identifier "MvPnC".

The use of Vendor Class Identifier DHCPv4 option 60 with specific value MvPnC is illustrated in table 4.1.1.2.

Table 4.1.1.2: Use of Vendor Class Identifier

Code	Length	Vendor Class Identifier				
60	5	M	v	P	n	C

The NE may alternatively identify itself by using the Vendor-Identifying Vendor Class DHCPv4 option 124 as specified RFC 3925 [4]. This option contains one or more Vendor-Identifying Vendor class information each identified by Enterprise Number as registered with IANA [7]. The format of Vendor-Identifying Vendor Class shall follow the rules specified in clause 3 of RFC 3925 [4], which is illustrated in table 4.1.1.3:

Table 4.1.1.3: Format of Vendor-Identifying Vendor Class

Code	Length 1-255	Enterprise Number 1	Vendor Class Data 1		Enterprise Number 2	Vendor Class Data 2		…
			Data Length 1	Opaque data 1		Data Length 2	Opaque data 2	…
124	**n**	**x**	**n**	**Data**	**y**	**n**	**Data**	…
octet	octet	4 octets	octets	n octets	4 octets	octet	n octets	

The NE may identify itself as MvPnC compatible DHCPv4 client using DHCPv4 option 124 in the following way:

- DHCPv4 option code 124;
- Vendor enterprise number 10415 for "3GPP";
- Vendor class data length 5 bytes;
- Vendor class data "MvPnC".

The use of Vendor- Identifying Vendor Class DHCPv4 option 124 with specific value MvPnC is illustrated in table 4.1.1.4.

Table 4.1.1.4: Use of Vendor-Identifying Vendor Class

Code	Length 1-255	Enterprise Number 1	Vendor Class Data 1						…
			Data Length 1	Opaque data 1					…
124	**n**	**10415**	**5**	**M**	**v**	**P**	**n**	**C**	**...**
octet	octet	4 octets	octet	octet	octet	octet	octet	octet	…

The order of vendor-identifying vendor class contained in option 124 does not matter, and any other vendor-identifying vendor class data with a different IANA enterprise number, if required by the vendor, may appear before or after the 3GPP vendor class.

4.1.2 DHCPv6

This clause describes DHCP options for use with DHCP for IPv6 (DHCPv6) that NE uses to identify itself in DHCP requests in Plug and Connect (PnC).

The NE performing the Initial IP Autoconfiguration procedure specified in clause 5.2 of 3GPP TS 28.315 [3], using IPv6 based network stack, shall identify itself using the Vendor Class DHCPv6 option 16 as specified in RFC 8415 [5]. The format of Vendor Class shall follow the rules specified in clause 21.16 of RFC 8415 [5], which is illustrated in table 4.1.2.1:

Table 4.1.2.1: Format of Vendor Class

Code	Length	Enterprise Number	Vendor Class Data				
			Vendor Class Length 1	Opaque Data 1	Vendor Class Length 2	Opaque Data 2	…
16	**n**	**x**	**n**	**Data**	**n**	**Data**	**…**
2 octets	2 octets	4 octets	2 octets	n octets	2 octets	n octets	…

The NE may identify itself as MvPnC compatible DHCPv6 client by using the Vendor Class DHCPv6 option 16 in the following way:

- DHCPv6 option code 16;
- Data length 11 bytes;
- Vendor enterprise number 10415 for "3GPP"
- Vendor class length 5 bytes;
- Vendor class data "MvPnC".

The use of Vendor Class DHCPv6 option 16 with specific value MvPnC is illustrated in table 4.1.2.2.

Table 4.1.2.2: Use of Vendor Class

Code	Length	Enterprise Number	Vendor Class Data					
			Vendor Class Length 1	Opaque data 1				
16	11	10415	5	M	v	P	n	C
2 octets	2 octets	4 octets	2 octets	octet	octet	octet	octet	octet

4.2 Entities information in DHCP replies

4.2.1 DHCPv4

This clause describes DHCP options for use with DHCP for IPv4 (DHCPv4) to send configuration information to NE in DHCP replies in Plug and Connect (PnC).

The information that NE receives from the DHCPv4 server while performing the Initial IP Autoconfiguration procedure specified in clause 5.2 of 3GPP TS 28.315 [3], using IPv4 based networking stack, may be classified in two categories: basic IP configuration and vendor specific configuration.

The basic IP configuration information is documented in RFC 2131 [8] and RFC 2132 [6] and may include the following:

- IP address ("yiaddr" field in [8]);
- Subnet Mask (option 1 in [6]);
- Router(s) (option 3 in [6]);
- IP address(es) of the DNS server(s) (option 6 in [6]);
- Domain Name (option 15 in [6]).

The vendor specific configuration is described in detail in clauses 4.2.3, 4.2.4 and 4.2.5.

The DHCPv4 option "Vendor Specific Information" specified in the clause 8.4 of RFC 2132 [6] is used as an opaque container carrying the vendor specific configuration from the DHCPv4 server to the NE performing the PnC procedure. The format of Vendor Specific Information shall follow the rules specified in clause 8.4 of RFC 2132 [6].

The use of Vendor Specific Information DHCPv4 option 43 for PnC is illustrated in table 4.2.1.1.

Table 4.2.1.1: Use of the Vendor Specific Information

Code	Length 1-255	Vendor Specific Information						
		Configuration attribute 1			Configuration attribute 2			...
43	n	Type1	Length1	Data	Type2	Length2	Data	...
octet	octet	octet	octet	n octets	octet	octet	n octets	...

The DHCPv4 option 43 may be used to carry MvPnC specific configuration from DHCPv4 server to the NE which identifies itself as MvPnC compatible DHCPv4 client using DHCPv4 option 60 as specified in the clause 4.1.1 of the present document. The MvPnC specific configuration is encoded in the field of "Vendor Specific Information" in table 4.2.1.1.

Alternatively, the DHCPv4 option "Vendor-Identifying Vendor Specific Information" specified in the clause 4 of RFC 3925 [4] is used as an opaque container carrying the Vendor specific configuration from the DHCPv4 server to the NE performing the PnC procedure. The option contains one or more Vendor Specific Information each identified by Enterprise Number. The format of Vendor-Identifying Vendor Specific Information shall follow the rules specified in clause 4 of RFC 3925 [4].

The use of Vendor-Identifying Vendor Specific Information DHCPv4 option 125 for PnC is illustrated in table 4.2.1.2.

Table 4.2.1.2: Use of Vendor-Identifying Vendor Specific Information

Code	Length 1-255	Enterprise Number 1	Data Length 1	Vendor Specific Information					Enterprise Number 2	…
125	n	x	n	Configuration Attribute 1			Configuration Attribute 2	…		
				sub-opt code 1	Subopt-len 1	Sub-option-data 1	…	…	y	…
octet	octet	4 octets	octet	octet	octet	n octets	…	…	4 octets	…

The DHCPv4 option 125 may be used to carry MvPnC specific configuration corresponding to 3GPP registered IANA Enterprise Number from DHCPv4 server to the NE which identifies itself as MvPnC compatible DHCPv4 client using DHCPv4 option 124 as specified in the clause 4.1.1 of the present document. Other vendor specific configuration with a different IANA enterprise number, if required by the vendor, may appear before or after the 3GPP MvPnC specific configuration.

The use of Vendor-Identifying Vendor Specific Information DHCPv4 option 125 with 3GPP registered IANA Enterprise Number for MvPnC is illustrated in table 4.2.1.3.

Table 4.2.1.3: Use of Vendor-Identifying Vendor Specific Information for MvPnC

Code	Length 1-255	Enterprise Number 1	Data Length 1	Vendor Specific Information (MvPnC Specific Configuration)					Enterprise Number 2	…
125	n	10415	n	Configuration Attribute 1			Configuration attribute 2	…		
				sub-opt code 1	Subopt-len 1	Sub-option-data 1	…	…	y	…
octet	octet	4 octets	octet	octet	octet	n octets	…	…	4 octets	…

If the size of vendor specific configuration contained in "Vendor Specific Information" option 43 and "Vendor-Identifying Vendor Specific Information" option125 is greater than 255 bytes, the RFC 3396 [9] encoding is used.

To avoid ambiguity in the interpretation of string vendor specific configuration attributes, the ASCII character encoding shall be used.

Standard network byte order shall be used with appropriate conversion function at the NE (matching the local little-endian / big-endian byte order).

Some vendor specific configuration attributes may be missing (e.g. the SeGW FQDN attribute may be not present if the SeGW IP address is present) or just have zero length (type octet followed by length octet with value zero and no data octets).

The qualifiers identifying which attributes are mandatory, Optional (O), Conditional Mandatory (CM) or Conditional Optional (CO) and corresponding conditions are defined it the clauses 4.2.3, 4.2.4 and 4.2.5.

The order of vendor specific configuration attribute is not important (e.g. attribute of type or subopt-code "1" may appear after the attribute type or subopt-code "5").

4.2.2 DHCPv6

This clause describes DHCP options for use with DHCP for IPv6 (DHCPv6) to send configuration information to NE in DHCP replies in Plug and Connect (PnC).

The information that NE receives from the DHCPv6 server while performing the Initial IP Autoconfiguration procedure specified in clause 5.2 of 3GPP TS 28.315 [3], using IPv6 based networking stack, may be classified in two categories: basic IP configuration and vendor specific configuration.

The NE acquires its IP address can either through stateful or stateless IP autoconfiguration. If IPv6 Stateless Address Autoconfiguration (SLAAC), as specified in clause 5.5 of RFC 4862 [13], is used for Initial IP Autoconfiguration, DHCPv6 is used in stateless mode.

The basic IP configuration information is documented in RFC 8415 [5] and RFC 3646 [10] and may include the following:

- IP address (option 3 as per clause 21.4 and option 5 as per clause 21.6 in [5], when DHCPv6 is not used in stateless mode)
- IP address(es) of the DNS server(s) (option 23 in [10]);
- Domain Name (option 24 in [10]).

The vendor specific configuration is described in detail in clauses 4.2.3, 4.2.4 and 4.2.5.

The DHCPv6 option "Vendor Specific Information" specified in the clause 21.17 of RFC 8415 [5] is used as an opaque container carrying the vendor specific configuration from the DHCPv6 server to the NE performing the PnC procedure. The format of Vendor Specific Information shall follow the rules specified in clause 21.17 of RFC 8415 [5].

The use of Vendor Specific Information DHCPv6 option 17 for PnC is illustrated in table 4.2.2.1.

Table 4.2.2.1: Use of the Vendor Specific Information

Code	Length	Enterprise Number	Vendor Specific Information						
			Configuration attribute 1			Configuration attribute 2			...
17	n	x	sub-opt code 1	Subopt-len 1	Sub-option-data 1	sub-opt code 2	Subopt-len 2	Sub-option-data 2	...
2 octets	2 octets	4 octets	2 octets	2 octets	n octets	2 octets	2 octets	n octets	...

The DHCPv6 option 17 may be used to carry MvPnC specific configuration corresponding to 3GPP registered IANA Enterprise Number from DHCPv6 server to the NE which identifies itself as MvPnC compatible DHCPv6 client using DHCPv6 option 16 as specified in the clause 4.1.2 of the present document.

The use of Vendor Specific Information DHCPv6 option 17 with 3GPP registered IANA Enterprise Number for MvPnC is illustrated in table 4.2.2.2.

Table 4.2.2.2: Use of the DHCPv6 Vendor Specific Information for MvPnC

Code	Length	Enterprise Number	Vendor Specific Information (MvPnC Specific Configuration)						
			Configuration attribute 1			Configuration attribute 2			...
17	n	10415	sub-opt code 1	Subopt-len 1	Sub-option-data 1	sub-opt code 2	Subopt-len 2	Sub-option-data 2	...
2 octets	2 octets	4 octets	2 octets	2 octets	n octets	2 octets	2 octets	n octets	...

If the size of vendor specific configuration contained in "Vendor Specific Information" option 17 is greater than 255 bytes, the RFC 3396 [9] encoding is used.

To avoid ambiguity in the interpretation of string vendor specific configuration attributes, the ASCII character encoding shall be used.

Standard network byte order shall be used with appropriate conversion function at the NE (matching the local little-endian / big-endian byte order).

Some vendor specific configuration attributes may be missing (e.g. the SeGW FQDN attribute may be not present if the SeGW IP address is present) or just have zero length (type octet followed by length octet with value zero and no data octets).

The qualifiers identifying which attributes are mandatory, Optional (O), Conditional Mandatory (CM) or Conditional Optional (CO) and corresponding conditions are defined it the clauses 4.2.3, 4.2.4 and 4.2.5.

The order of vendor specific configuration attribute is not important (e.g. subopt-code "1" may appear after the subopt-code "5").

4.2.3 Certification Authority (CA/RA) server

This clause specifies the information about Certification Authority server that NE receives from DHCP server in Initial IP Autoconfiguration procedure specified in clause 5.2 of 3GPP TS 28.315 [3] and uses for Certificate Enrolment procedure. The CA/RA configuration attributes are specified in Table 4.2.3.1. The attribute tag (code) is vendor specific. The attribute tag (code) value specified in the table 4.2.3.1 is only expected in MvPnC specific configuration as specified in the clauses of 4.2.1 and 4.2.2 in DHCP replies to the NE which identifies itself as MvPnC compatible DHCP client.

Table 4.2.3.1: CA/RA configuration attributes

Attribute name	Attribute tag (code)	Attribute length	Attribute qualifier	Attribute description
IP address of the CA/RA	01	Variable	CO	IP address of the CMP server. An IPv4 IP address is represented as 4 octets. An IPv6 IP address is represented as 16 octets.
FQDN of the CA/RA	02	Variable	CO	ASCII string representing the Fully Qualified Domain Name of the CMP server. In case the FQDN is used, the IP address of the DNS server needs to be made available to the NE before certificate enrolment.
Port number of the CA/RA	03	Variable	M	Integer representing the port number used by CMP server. The port for HTTP/HTTPSs transfer of CMP messages is not explicitly given in RFC 6712 [12], therefore this parameter is required. The port number is usually represented as 2 octets.
Path to the CA/RA directory	04	Variable	M	ASCII string representing the path to the CMP server directory. A CMP server may be located in an arbitrary path other than root.
Subject name of the CA/RA	05	Variable	M	ASCII string representing the subject name of the CA/RA. The use is described in 3GPP TS 33.310 [11] clause 9.5.3.
Protocol indication	06	Variable	CM	ASCII string representing the protocol (HTTP or HTTPS) to be used for certificate enrolment. The use is described in 3GPP TS 33.310 [11] clause 9.6.

Table 4.2.3.2: Attribute constraints

Name	Definition
IP address CO qualifier	The IP address is optional if the FQDN is present
FQDN CO qualifier	The FQDN is optional if the IP address is present
Protocol indication CM qualifier	The protocol indication is mandatory if HTTPS protocol is used

4.2.4 Security Gateway (SeGW)

This clause specifies the information about Security Gateway server that NE receives from DHCP server in Initial IP Autoconfiguration procedure specified in clause 5.2 of 3GPP TS 32.508 [5] and uses for Establishing Secure Connection procedure. The Security Gateway configuration attributes are specified in Table 4.2.4.1. The attribute tag (code) is vendor specific. The attribute tag (code) value specified in the table 4.2.4.1 is only expected in MvPnC specific configuration as specified in the clauses of 4.2.1 and 4.2.2 in DHCP replies to the NE which identifies itself as MvPnC compatible DHCP client.

Table 4.2.4.1: Security Gateway configuration attributes

Attribute name	Attribute tag (code)	Attribute length	Attribute qualifier	Attribute description
IP address of the SeGW	07	Variable	CO	IP address of the Security Gateway. An IPv4 IP address is represented as 4 octets. An IPv6 IP address is represented as 16 octets.
FQDN of the SeGW	08	Variable	CO	ASCII string representing the Fully Qualified Domain Name of the Security Gateway. In case the FQDN is used, the IP address of the DNS server needs to be made available to the NE before establishing secure connection.

Table 4.2.4.2: Attribute constraints

Name	Definition
IP address CO qualifier	The IP address is optional if the FQDN is present
FQDN CO qualifier	The FQDN is optional if the IP address is present

4.2.5 Software Configuration Server (SCS)

This clause specifies the information about SCS that NE receives either from DHCP server in Initial IP Autoconfiguration procedure specified in clause 5.2 of 3GPP TS 28.315 [3] or from secure DHCP server in Establishing Connection to SCS procedure specified in clause 5.5 of 3GPP TS 28.315 [3] and uses for Establishing Connection to SCS procedure. The SCS configuration attributes are specified in Table 4.2.5.1. The attribute tag (code) is vendor specific. The attribute tag (code) value specified in the table 4.2.5.1 is only expected in MvPnC specific configuration as specified in the clauses of 4.2.1 and 4.2.2 in DHCP replies to the NE which identifies itself as MvPnC compatible DHCP client.

Table 4.2.5.1: SCS configuration attributes

Attribute name	Attribute tag (code)	Attribute length	Attribute qualifier	Attribute description
IP address of the EM	09	Variable	CO	IP address of the SCS. An IPv4 IP address is represented as 4 octets. An IPv6 IP address is represented as 16 octets.
FQDN of the EM	10	Variable	CO	ASCII string representing the Fully Qualified Domain Name of the SCS. In case the FQDN is used, the IP address of the DNS server needs to be made available to the NE before establishing connection to the SCS.

Table 4.2.5.2: Attribute constraints

Name	Definition
IP address CO qualifier	The IP address is optional if the FQDN is present
FQDN CO qualifier	The FQDN is optional if the IP address is present

4.3 Entities Fully Qualified Domain Names (FQDN)

4.3.1 General

This clause describes the Fully Qualified Domain Names (FQDNs) used in Plug and Connect (PnC) procedures.

The FQDNs used in PnC are in the form of a domain name as specified in IETF RFC 1035 [15].

The sub-domains used in PnC are allocated within the ".3gppnetwork.org" domain.
The GSM Association is in charge of allocating the new sub-domains of ".3gppnetwork.org" domain name.
The procedure specified in Annex E of 3GPP TS 23.003 [14] is used for the sub-domain allocation.

The FQDNs used in PnC follow the general encoding rules specified in clause 19.4.2.1 of 3GPP TS 23.003 [14].

The format of FQDNs used in PnC follows the "<vendor ID>.<system>.<OAM realm>" pattern.

NOTE: Where "<vendor ID>.<system>.oam" represents the <service_id> shown in the first row of table E.1 of 3GPP TS 23.003 [14].

The <vendor ID> label is optional and is required in the operator deployments where multiple instances of a particular network entity type are not provided by the same vendor. If present, the <vendor ID> label is in the form "vendor<ViD>", where <ViD> field corresponds to the ID of the vendor. The specific deployment scenario (e.g. one network entity instance per vendor or one network entity instance for all vendors) is not known to the NE when it connects to the network. Therefore, it should first try to resolve the FQDN containing the <vendor ID> label and if it fails, try to resolve the FQDN without the <vendor ID> label.

The details of the <system> label are described in clauses 4.3.2, 4.3.3 and 4.3.4.

The <OAM realm> label is the operator's OAM realm domain name in the form of "oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org", where "<MNC>" and "<MCC>" fields correspond to the MNC and MCC of the operator's PLMN. Both the "<MNC>" and "<MCC>" fields are 3 digits long. If the MNC of the PLMN is 2 digits, then a zero shall be added at the beginning.

An example of an OAM realm domain name is:

```
MCC = 123;
MNC = 45;
```

Which gives the OAM realm domain name: "`oam.mnc045.mcc123.3gppnetwork.org`".

4.3.2 Certification Authority (CA/RA) server

The Certification Authority server (CA/RA) FQDN is derived as follows. The "`cara`" <system> label is added in front of the operator's OAM realm domain name:

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

If particular operator deployment scenario has multiple CA/RA servers (one per vendor), the <vendor ID> label is added in front of the "`cara`" label:

```
vendor<ViD>.cara.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

An example of a CA/RA FQDN is:

```
MCC = 123;
MNC = 45;
ViD = abcd;
```

Which gives the CA/RA FQDN: "`cara.oam.mnc045.mcc123.3gppnetwork.org`" and "`vendorabcd.cara.mnc045.mcc123.3gppnetwork.org`".

4.3.3 Security Gateway (SeGW)

The Security Gateway (SeGW) FQDN is derived as follows.
The "segw" <system> label is added in front of the operator's OAM realm domain name:

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

If particular operator deployment scenario has multiple Security Gateways (one per vendor), the <vendor ID> label is added in front of the "segw" label:

```
vendor<ViD>.segw.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

An example of a SeGW FQDN is:

```
MCC = 123;

MNC = 45;

ViD = abcd;
```

Which gives the SeGW FQDN: "segw.oam.mnc045.mcc123.3gppnetwork.org" and "vendorabcd.segw.mnc045.mcc123.3gppnetwork.org".

4.3.4 Software Configuration Server (SCS)

The SCS FQDN is derived as follows:
The "scs" <system> label is added in front of the operator's OAM realm domain name:

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

If a particular operator deployment scenario has multiple SCSs (one per vendor), the <vendor ID> label is added in front of the "scs" label:

```
vendor<ViD>.scs.oam.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

An example of a SCS FQDN is:

```
MCC = 123;

MNC = 45;

ViD = abcd;
```

Which gives the SCS FQDN: "scs.oam.mnc045.mcc123.3gppnetwork.org" and "vendorabcd.scs.mnc045.mcc123.3gppnetwork.org".

SCS can be element manager (EM), for example in IRP based architecture, "em" system label is added in front of the operator's OAM realm domain name, an example of an EM FQDN is:

"em.oam.mnc045.mcc123.3gppnetwork.org" and "vendorabcd.em.mnc045.mcc123.3gppnetwork.org".

Annex A (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2021-06	SA5#137-e	S5-213664					0.1.0
2021-12	SA5#140-e	S5-216604					0.2.0
2022-01	SA5#141-e	S5-221750					0.3.0
2022-03	SA#95e	SP-220124				Presented for information and approval	1.0.0
2022-03	SA#95e					Upgrade to change control version	17.0.0

History

Document history		
V17.0.0	May 2022	Publication