

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.369

(06/2008)

SERIES J: CABLE NETWORKS AND TRANSMISSION
OF TELEVISION, SOUND PROGRAMME AND OTHER
MULTIMEDIA SIGNALS

IPCablecom

IPCablecom2 E-UE provisioning framework specification

Recommendation ITU-T J.369

Document ID: 123456789

Recommendation ITU-T J.369

IPCablecom2 E-UE provisioning framework specification

Summary

Recommendation ITU-T J.369 specifies the network and protocol requirements to configure and manage IPCablecom2 Embedded User Equipment (E-UE) along with the associated users and applications.

Source

Recommendation ITU-T J.369 was approved on 13 June 2008 by ITU-T Study Group 9 (2005-2008) under Recommendation ITU-T A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

...

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
2.1	Normative references.....	1
2.2	Informative references.....	3
2.3	Reference acquisition	3
3	Terms and definitions	3
4	Abbreviations, acronyms and conventions	4
4.1	Abbreviations and acronyms	4
4.2	Conventions.....	4
5	Technical overview.....	5
5.1	Embedded User Equipment (E-UE)	5
5.2	Provisioning.....	5
5.3	Reuse of IP Cablecom Device Provisioning	5
5.4	IP Network Environments	6
5.5	E-UE Provisioning Model	6
5.6	E-UE Provisioning Data Model.....	8
6	E-UE provisioning framework	8
6.1	eUE Provisioning Interfaces.....	8
6.2	E-UE Provisioning Components	11
6.3	E-UE Provisioning Flows.....	13
6.4	E-UE Configuration.....	31
6.5	E-UE Management	33
6.6	E-UE Additional features	33
Annex A	– eUE Capabilities.....	35
A.1	eUE Capabilities.....	35
A.2	Capability Enhancements	35

Recommendation ITU-T J.369

IPCablecom2 E-UE provisioning framework specification

1 Scope

This Recommendation describes the provisioning mechanism for IPCablecom2 Embedded User Equipment (E-UE). The purpose is to specify the network and protocol requirements to configure and manage E-UEs, along with the associated users and applications. The configuration and management data requirements are specified in a related document, the E-UE Provisioning Data Models Specification [PKT-EUE-DATA].

The configuration and management of non-embedded UEs such as software-based clients, and network elements such as the CSCFs and the HSS, is out of scope for this Recommendation.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

NOTE – The structure and content of this Recommendation have been organized for ease of use by those familiar with the original source material; as such, the usual style of ITU-T Recommendations has not been applied.

2 References

2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- | | |
|--------------------|--|
| [CL-BB-MIB] | Recommendation ITU-T J.199: <i>Battery backup for cable-based devices.</i> |
| [CL-CANN-DHCP-Reg] | Recommendation ITU-T J.166: <i>IPCablecom Management Information Base (MIB) framework Annex A.</i> |
| [DOCSIS-RFI] | Recommendation ITU-T J.112: <i>Transmission systems for interactive cable television services.</i> |
| [eDOCSIS] | Recommendation ITU-T J.126: <i>Embedded Cable Modem device specification.</i> |
| [PKT-PROV1.5] | Recommendation ITU-T J.167: <i>Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems.</i> |
| [PKT-SEC1.5] | Recommendation ITU-T J.170: <i>IPCablecom security specification.</i> |
| [PKT-MEM1.5] | Recommendation ITU-T J.172: <i>IPCablecom management event mechanism.</i> |

[PKT-EUE-DATA]	Recommendation ITU-T J.370: <i>IP Cablecom2 Provisioning data model Specification</i> .
[RFC 1034]	RFC1034/STD0013, <i>Domain names – concepts and facilities</i> , November 1987.
[RFC 1035]	RFC1035/STD0013, <i>Domain names – implementation and specification</i> , November 1987.
[RFC 1350]	IETF RFC 1350/STD0033, <i>The TFTP protocol (Revision 2)</i> , July 2003.
[RFC 2131]	IETF RFC 2131, <i>DHCP: Dynamic Host Configuration Protocol</i> , March 1997.
[RFC 2234]	IETF RFC 2234, <i>Augmented BNF for Syntax Specifications: ABNF</i> , November 1997.
[RFC 2246]	IETF RFC 2246, <i>The TLS Protocol Version 1.0</i> , January 1999.
[RFC 2461]	IETF RFC 2461, <i>Neighbor Discovery for IP Version 6 (IPv6)</i> , December 1998.
[RFC 2462]	IETF RFC 2462, <i>IPv6 Stateless Address Autoconfiguration</i> , December 1998.
[RFC 2616]	IETF RFC 2616, <i>Hypertext Transfer Protocol – HTTP/1.1</i> , June 1999.
[RFC 2782]	IETF RFC 2782, <i>A DNS RR for specifying the location of services (DNS SRV)</i> , February 2000.
[RFC 2915]	IETF RFC 2915, <i>The Naming Authority Pointer (NAPTR) DNS Resource Record</i> , September 2000.
[RFC 3164]	IETF RFC 3164, <i>BSD Syslog protocol</i> , August 2001.
[RFC 3268]	IETF RFC 3268, <i>Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)</i> , June 2002.
[RFC 3315]	IETF RFC 3315, <i>Dynamic Host Configuration Protocol for IPv6 (DHCPv6)</i> , July 2003.
[RFC 3396]	IETF RFC 3396, <i>Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)</i> , November 2002.
[RFC 3411]	IETF RFC 3411/STD0062, <i>An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks</i> .
[RFC 3413]	IETF RFC 3413/STD0062, <i>Simple Network Management Protocol (SNMP) Applications</i> , December 2002.
[RFC 3414]	IETF RFC 3414/STD0062, <i>User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)</i> , December 2002.
[RFC 3495]	IETF RFC 3495, <i>Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration</i> , March 2003.
[RFC 3513]	IETF RFC 3513, <i>Internet Protocol Version 6 (IPv6) Addressing Architecture</i> , April 2003.
[RFC 3584]	IETF RFC 3584, <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i> , August 2003.

- [RFC 3594] IETF RFC 3594, *PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option*, September 2003.
- [RFC 3596] IETF RFC 3596, *DNS Extensions to Support IP Version 6*, October 2003.
- [RFC 3617] IETF RFC 3617, *Uniform Resource Identifier (URI) Scheme and Applicability Statement for the Trivial File Transfer Protocol (TFTP)*, October 2003.
- [RFC 3925] IETF RFC 3925, *Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)*, October 2004.
- [RFC 4291] IETF RFC 4291, *IP Version 6 Addressing Architecture*, February 2006.
- [RFC 4361] IETF RFC 4361, *Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)*, February, 2006.
- [RFC 4704] IETF RFC 4704, *The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client*, October 2006.

2.2 Informative references

This Recommendation uses the following informative references.

- [PKT-ARCH-TR] Recommendation ITU-T J.160: *Architectural framework for the delivery of time-critical services over cable television networks using cable modems*.
- [PKT-24.229] Recommendation ITU-T J.366.4 (draft): *IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification*.
- [RFC 3319] IETF RFC 3319, *H. Schulzrinne, B. Volz, Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers*, July 2003.

2.3 Reference acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; <http://www.cablelabs.com>.
- Internet Engineering Task Force (IETF) Secretariat, 46000 Center Oak Plaza, Sterling, VA 20166, Phone +1-571-434-3500, Fax +1-571-434-3535, <http://www.ietf.org/>.

3 Terms and definitions

This Recommendation defines the following terms:

- 3.1 configuration:** Configuration is the process of defining and propagating data to network elements for providing services.
- 3.2 data model:** An abstract model that describes representation of data in a system.
- 3.3 eCM:** The logical DOCSIS CM component of a E-UE, complies with DOCSIS, eDOCSIS and IPCablecom requirements.
- 3.4 eUE:** The logical IPCablecom UE component of a E-UE, complies with eSAFE and IPCablecom requirements.
- 3.5 embedded user equipment (E-UE):** A single physical device embedded with an eDOCSIS-compliant DOCSIS Cable Modem and an IPCablecom eUE.

3.6 Kerberos: Authentication protocol allowing one network entity (Client) to be mutually authenticated to another one (Application Server) using the "Kerberos ticket" retrieved by the Client from a dedicated Authentication Server (KDC).

3.7 provisioning: Provisioning refers to the processes involved in the initialization of user attributes and resources to provide services to a User. This involves protocols, methodologies, and interfaces to network elements such as: Order Entry and Workflow Systems that carry out business processes, Operational Support Elements that handle network resources, Application Servers that offer services and User Equipment that offer services, among others.

4 Abbreviations, acronyms and conventions

4.1 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

CODEC	COding-DECoding algorithms used to compress/decompress the data representing the Voice (or Video) media traffic
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
KDC	Key Distribution Center: the Authentication Server which implements the Kerberos PKINIT Authentication Protocol
MIB	Management Information Base
MSO	Multiple System Operator (A network operator)
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SYSLOG	System Logging Protocol – a protocol which defines the transport mechanism for the messages carrying various logging information
TFTP	Trivial File Transfer Protocol
TGT	Ticket Granting Ticket
ToD	Time of the Day – the network protocol which delivers the time of the day to a network client from the Time Of the Day from the network server
UE	User Equipment

4.2 Conventions

Throughout this Recommendation, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word means that the item is an absolute requirement of this Recommendation.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this Recommendation.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

5 Technical overview

The framework specified for configuration and management in this Recommendation reuses the protocols and interfaces specified for Embedded Multimedia Terminal Adaptors (E-MTAs) in the IP-Cablecom Device Provisioning specification [PKT-PROV1.5]. As such, this Recommendation presents a specific profile of the IP-Cablecom Device Provisioning solution. In addition, it enhances device provisioning to address additional requirements that are in scope for eUEs, but not eMTAs. Specifically, eUEs connect to the IP-Cablecom architecture based on SIP and the IMS, and support IPv6. The following subclauses provide more details on E-UEs, the reuse of Device Provisioning, and related aspects.

5.1 Embedded User Equipment (E-UE)

IP-Cablecom is based on SIP and IMS, and aims to support a wide variety of clients such as embedded eDOCSIS clients (e.g., telephony devices), non-embedded clients (e.g., dual-mode handsets), and software-based clients. Consistent with the IMS, IP-Cablecom clients are termed User Equipment (UE). For more information about UEs in IP-Cablecom, please refer to the IP-Cablecom Architecture Framework Technical Report ([PKT-ARCH-TR]).

This Recommendation considers only one family of UEs – those embedded with a DOCSIS Cable Modem, termed E-UE. Specifically, the E-UE is a single physical device embedded with an eDOCSIS-compliant DOCSIS Cable Modem (eCM) and an eUE that complies with eDOCSIS, eSAFE, and IP-Cablecom UE requirements. Consistent with eDOCSIS terminology, the logical DOCSIS and UE components are referenced by the terms eCM and eUE, respectively. For more information about eDOCSIS, please refer to the eDOCSIS specification ([eDOCSIS]).

It is to be noted that the term "DOCSIS" in this Recommendation is understood to refer to DOCSIS version 1.1 or later unless explicitly stated otherwise. Please refer to the corresponding DOCSIS specifications for more information about DOCSIS (for instance, DOCSIS 1.1 is specified in [DOCSIS-RFI] and associated specifications).

5.2 Provisioning

Provisioning refers to the processes involved in the initialization of the attributes and resources on clients and network components to provide services to a user. The term Provisioning, in this Recommendation, refers to the process of configuration and readiness for management of E-UEs. Configuration is generally specified as the process of defining and transporting the provisioning data to the network elements providing services. Management refers to the protocols, methodologies and interfaces that enable monitoring, and the control and availability of the offered services in an Operator's Network.

5.3 Reuse of IP-Cablecom Device Provisioning

IP-Cablecom Device Provisioning is a configuration and management solution designed for embedded IP-Cablecom devices, specifically the IP-Cablecom Embedded Multimedia Terminal Adaptors (E-MTAs). It is based on IETF standards and protocols such as SNMP ([RFC3411]),

DHCP ([RFC2131]), and TFTP ([RFC1350]). This is currently being used by network operators for IP-Cablecom deployments.

To reuse the existing OSS infrastructure and to expedite roll out of E-UEs with minimal OSS changes, this Recommendation offers a framework that reuses the protocols and interfaces specified by IP-Cablecom Device Provisioning with enhancements to support IP-Cablecom E-UEs. The enhancements include:

- Support for IPv6 eUEs.
- Support for eUEs connecting to an IP-Cablecom network.

To minimize the restating of requirements, this Recommendation makes numerous references to [PKT-PROV1.5], with the following clarifications.

- All requirements regarding Telephony Services are not applicable and will be ignored.
- Any IP-Cablecom Signalling requirements (e.g., endpoint provisioning for CMSs), are not applicable to eUEs.
- Requirements for the E-MTA or eMTA will be interpreted as requirements for E-UE and eUE, respectively, in referenced clauses.
- All references to data definitions, such as the MTA MIB, will be interpreted in accordance with [PKT-EUE-DATA] and explicit data requirements in this Recommendation.
- For any conflict in requirements, this Recommendation will always take precedence over [PKT-PROV1.5].

5.4 IP Network Environments

Given their embedded nature, E-UEs will always connect via a DOCSIS network. Thus, the DOCSIS Operator controls the IP network connectivity and IP parameters such as IP address information. Further, IP-Cablecom supports E-UEs that can be IPv4, IPv6, or both. This Recommendation allows for the specified IP network versions, and allows for a choice between IPv4 and IPv6 for the eUE when the eCM is provisioned. This is an enhancement for IP-Cablecom Device Provisioning, which only handles IPv4 eSAFE clients.

5.5 E-UE Provisioning Model

E-UE Provisioning supports static and dynamic configuration of E-UEs. Static configuration is specified as a pre-established set of configuration parameters for an E-UE that is pre-configured in the Operator's network. In contrast, dynamic configuration is characterized by the capability to create and provide configuration to E-UEs dynamically, even those that are not pre-configured in the Operator's network. Dynamic provisioning can be used to provide emergency or subscription-related information such as emergency dialing for voice services and self-subscription redirects. It is to be noted that support for dynamic configuration during any particular deployment is a choice left to the network operator.

The eCM component of an E-UE is governed by the DOCSIS specifications and any enhancements provided explicitly in this Recommendation, such as IP-Cablecom-specific DHCP options. The provisioning of the eUE is accomplished using the provisioning flows specified in this Recommendation. There are three kinds of eUE flows: Basic, Hybrid and Secure. A provisioning flow is selected when the eUE initializes and obtains its IP configuration information. The provisioning flow is deemed complete when the eUE obtains its configuration via a configuration file.

A high-level conceptual diagram highlighting all the components and the provisioning flows is indicated in Figure 1.

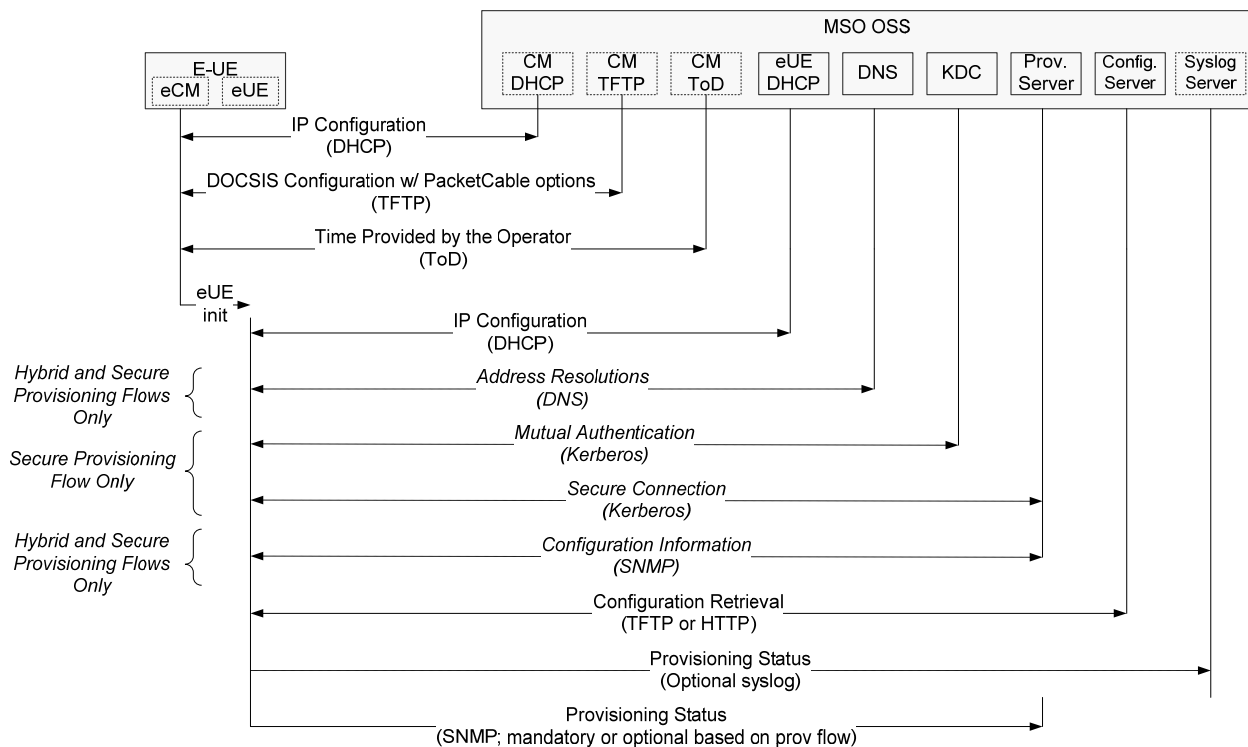


Figure 1 – IPCablecom E-UE Provisioning Flow (conceptual)

As indicated in Figure 1, the reset of an E-UE results in the eCM component being initialized first. Once the eCM has been provisioned, and if it obtains IPCablecom-specific parameters, the eUE is initialized. The eUE is then provided with IP configuration information that indicates the choice of provisioning flow.

Figure 1 also highlights various OSS components required for eUE provisioning. Their roles can be briefly summarized as follows:

DHCP Server

The DHCP server is used in all the provisioning flows and provides IP configuration information, such as the IP address and DNS server information. In addition, it is also used to provide IPCablecom-specific configuration, such as the choice of provisioning flow and network component information (e.g., Kerberos realm in the secure provisioning flow).

DNS Server

The DNS server is primarily used in the Hybrid and Secure provisioning flows and allows the eUE to discover the IP address of network components, such as the KDC and the Provisioning Server. The DNS server itself is obtained via DHCP as part of the IP configuration information.

KDC

The KDC is the authentication server specified by the Kerberos protocol. It is used for mutual authentication between the eUE and the network operator's network. It also facilitates mutual authentication between the E-UE and the Provisioning server, and with SNMPv3 connectivity establishment in the case of the secure provisioning flow.

Provisioning Server

The Provisioning Server containing the SNMP entity is used in the Hybrid and Secure provisioning flows to provide configuration to the eUE. In the case of the secure provisioning flow, this component also acts as a Kerberos Application Process.

It uses SNMP for configuration in the Hybrid and Secure Provisioning flows. In the secure mode, SNMPv3 is used to exchange authentication, and optional encryption, information related to the configuration file.

TFTP and HTTP Servers

TFTP and, optionally, HTTP servers can be used to propagate the configuration file to the eUE.

Syslog Server

Syslog Servers are used to collect management events from the client. To use syslog, the eUE needs to be configured with a valid Syslog Server and syslog enabled as a management event transport.

5.6 E-UE Provisioning Data Model

The IPCablecom provisioning data model allows for a many-to-many relationship among users, devices, and applications. For more information on the data model and any data elements referenced in this Recommendation, please refer to the IPCablecom E-UE Provisioning Data Models specification ([PKT-EUE-DATA]).

6 E-UE provisioning framework

This clause presents the normative requirements for the E-UE Provisioning Framework, based on IPCablecom Device Provisioning. It includes references to IPCablecom Device Provisioning, and any necessary enhancements to support IPCablecom E-UEs.

The framework aims to reuse all the IPCablecom Device Provisioning interfaces, and supports all three provisioning flows: Basic, Hybrid and Secure. For more information on IPCablecom Device Provisioning please refer to [PKT-PROV1.5].

Clause 6.1 presents the eUE Provisioning Interfaces. For provisioning an eCM embedded within an E-UE, please refer to [PKT-PROV1.5] and any enhancements specified in clause 6.2.1.1.

6.1 eUE Provisioning Interfaces

Figure 2 represents the network components and interfaces that form the eUE Provisioning Framework.

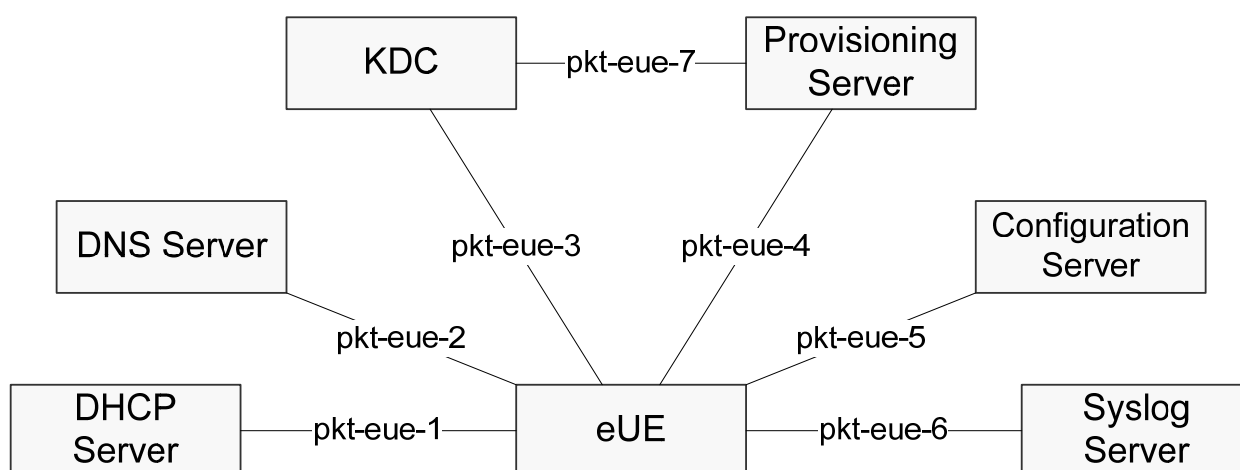


Figure 2 – E-UE Provisioning Components and Interfaces