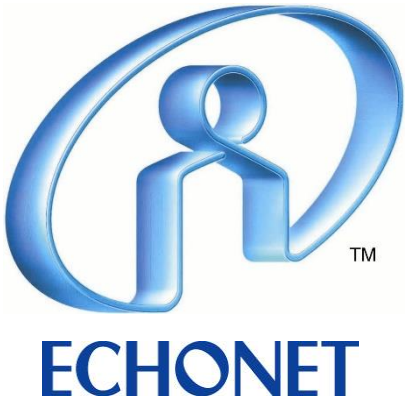
# ECHONET Lite System Design Guidelines

## 2nd edition



Revision History

・1st edition draft　May 23, 2018　Establishment, Disclosed to member companies only.
・Created by revising ECHONET Lite specifications Ver.1.12, Section 5.
・Added “Concept of implementation of manufacturer code properties” to Section 2.9.3.
・Moved “Guidelines on Handling Transmission-only Devices” to Section 2.10.
・Moved “Guidelines on TCP” to Section 2.11.
・Added “Implementation Cases and Policies on Smart Electric Energy Meters” as Chapter 6.

・1st edition　July 6, 2018　Published for general public
・Corrected clerical error in the name of the Interface Specification for Application Layer Communication between High-voltage Smart Electric Energy Meters and EMS Controllers

・2nd edition draft　April 5, 2019　Disclosed to member companies only.
・Added supplementary explanation regarding IGMP standards in Section 2.4.2
・Added supplementary explanation and figure 2-4 regarding identification number property to Section 2.8
・Created Section 2.12
・Corrected descriptions throughout Chapter 6.
・Corrected titles of Sections 6.2 and 6.3
・Added case studies to 6.2.1 (2)

・2nd edition　June 24, 2019　Published for the general public

## *Contents*

Revision History ..... ii
*Contents* ..... iii
Chapter 1 Introduction ..... 1-1
1.1 REFERENCE STANDARDS ..... 1-1
Chapter 2 Guidelines on the Implementation of ECHONET Lite ..... 2-1
2.1 GUIDELINES ON THE HANDLING OF PROPERTY VALUES ..... 2-1
2.2 GUIDELINES ON THE HANDLING OF RESPONSES ..... 2-3
2.3 GUIDELINES ON OPC ..... 2-4
2.4 GUIDELINES ON GENERAL BROADCAST ..... 2-4
2.4.1 Basic Concept ..... 2-4
2.4.2 Concept in an IPv4 environment ..... 2-4
2.5 GUIDELINES ON THE NUMBER OF INSTANCES ..... 2-6
2.6 GUIDELINES ON THE PROPERTY VALUE WRITE & READ SERVICE ..... 2-6
2.7 GUIDELINES ON SENDING MESSAGES ..... 2-6
2.8 GUIDELINES ON MANAGEMENT OF ECHONET LITE DEVICE ..... 2-7
2.9 GUIDELINES ON IMPLEMENTATION OF ECHONET PROPERTIES ..... 2-7
2.9.1 Concept of objects implemented in ECHONET Lite middleware adapters ..... 2-8
2.9.2 Concept of implementing operation status properties ..... 2-8
2.9.3 Concept of implementation of manufacturer code properties ..... 2-8
2.10 GUIDELINES ON HANDLING TRANSMISSION-ONLY DEVICES ..... 2-8
2.11 GUIDELINES ON TCP ..... 2-9
2.12 CAUTIONS REGARDING WIRELESS LAN NETWORKS ..... 2-10
Chapter 3 Guidelines for Secure Communications in ECHONET Lite ..... 3-1
3.1 OVERVIEW ..... 3-1
3.2 SECURE COMMUNICATIONS IN LOWER LAYERS ..... 3-1
3.2.1 DTLS ..... 3-1
3.2.2 IPsec ..... 3-2
3.2.3 RFC5191 ..... 3-2
3.2.4 AES-CCM ..... 3-2
3.2.5 WEP ..... 3-2
3.2.6 WPA ..... 3-2
3.2.7 WPA2 ..... 3-2
3.2.8 IEEE802.1X ..... 3-3
Chapter 4 Guidelines on Node Detection and Finding Procedure ..... 4-1

4.1 CONCEPT ..... 4-1
4.2 DETECTION BY MESSAGE SEND FROM NODE TO CONTROLLER ..... 4-1
4.3 FINDING BY MESSAGE SEND FROM CONTROLLER TO NODE ..... 4-1
4.4 CONFIRMATION OF ECHONET LITE DEVICE CONNECTIONS ..... 4-2

Chapter 5 Guidelines on Remote Control ..... 5-1

5.1 BASIC CONCEPT ..... 5-1
5.2 WHEN USING MIDDLEWARE ADAPTORS ..... 5-1

Chapter 6 Implementation Cases and Policies on Smart Electric Energy Meters ..... 6-1

6.1 IMPLEMENTATION CASES FOR SIMPLEX METERS ..... 6-1
6.2 IMPLEMENTATION CASES FOR "DAY FOR WHICH THE HISTORICAL DATA OF MEASURED CUMULATIVE AMOUNTS OF ELECTRIC ENERGY IS TO BE RETRIEVED" PROPERTY ..... 6-2
6.3 IMPLEMENTATION CASES FOR CUMULATIVE ELECTRIC ENERGY VALUE WHEN LACKING MEASURED DATA ..... 6-2
6.4 IMPLEMENTATION CASES ON LIVING CONFIRMATION METHOD ..... 6-3
6.5 IMPLEMENTATION CASE FOR RECONNECTION ATTEMPT ..... 6-4
6.6 IMPLEMENTATION CASE FOR STARTING ECHONET LITE COMMUNICATION ..... 6-5
6.7 IMPLEMENTATION CASE FOR REPLACING CONTROLLERS ..... 6-6
6.8 IMPLEMENTATION CASE ON HOW TO RESPOND TO HISTORICAL DATA ON CUMULATIVE AMOUNTS OF ELECTRIC ENERGY BEFORE ESTABLISHING A ROUTE B CONNECTION ..... 6-6
6.9 IMPLEMENTATION CASE ON ABNORMALITIES DURING PANA AUTHENTICATION ..... 6-7
6.10 IMPLEMENTATION CASE FOR MEASURED CUMULATIVE AMOUNT OF ELECTRIC ENERGY ..... 6-7
6.11 IMPLEMENTATION CASE FOR TAKING MEASURES AGAINST DOS ATTACK (1) ..... 6-8
6.12 IMPLEMENTATION CASE ON TAKING MEASURES AGAINST DOS ATTACK (2) ..... 6-8

# Chapter 1 Introduction

This book summarizes policies on the interpretation of standards and specifications, as well as system configurations and implementation to prevent product problems in the market, at Plug Fest, and at other events for the purpose of improving the interoperability of ECHONET Lite specifications and the application communication interface specifications of devices.

## 1.1 Reference Standards

Standards referenced in this document are as stated below. Matters not explicitly covered in this document shall comply with the standard documents.

[EL] The ECHONET Lite Specification
[APPENDIX] APPENDIX Detailed Requirements for Device objects
[LSM_AIF] Application Communication Interface Specifications between Low-voltage Smart Electric Energy Meters and HEMS Controllers
(Disclosed to member companies only)
[HSM_AIF] Application Communication Interface Specifications between High-voltage Smart Electric Energy Meters and HEMS Controllers
(Disclosed to member companies only)

# Chapter 2 Guidelines on the Implementation of ECHONET Lite

Inquiries about the interpretations of specifications received through Plugfest or other means are summarized in this chapter as guidelines.

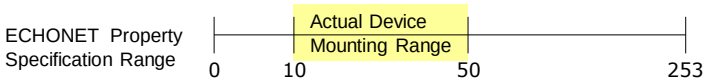
## 2.1 Guidelines on the Handling of Property Values

This section provides guidelines on handling cases where a previously set property value is within the ECHONET property definition range but is outside the range in which the corresponding actual device can operate.

(1) In a case where the continuous value range in which the actual device represented by an ECHONET property can operate is narrower than the ECHONET property definition range and a value has been set in the ECHONET property that falls between the upper and lower limit values for the ECHONET property but not between the upper and lower limit values for the actual device, it is recommended that the application software program in the ECHONET Lite node use the following as the property value for the actual device and the ECHONET property value:

The upper limit value for the actual device when the previously set value in the ECHONET property falls between the upper limit value for the ECHONET property and the upper limit value for the actual device; and the lower limit value for the actual device when the previously set value in the ECHONET property falls between the lower limit value for the ECHONET property and the lower limit value for the actual device.

For example, when the ECHONET property definition range is 0x00 to 0xFD (0°C to 253°C) and the operation range of the actual device represented by the ECHONET property is 0x0A to 0x32 (10°C to 50°C) and a value (e.g. 60°C) has been set in the ECHONET property that falls between the upper limit value for the actual device and the upper limit value for the ECHONET property, it is recommended that the upper limit value for the actual device (0x32 (50°C)) be used as the ECHONET property value. When a value (e.g. 5°C) has been set in the ECHONET property that falls between the lower limit value for the actual device and the lower limit value for the ECHONET property under the same range conditions, it is recommended that the lower limit value for the actual device (0x0A (10°C)) be used as the ECHONET property value. Fig. 2.1 illustrates these examples.

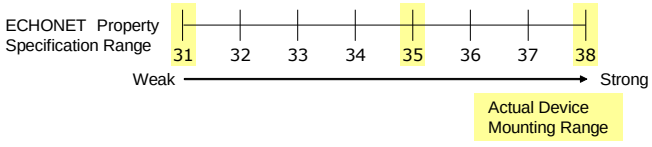



•When 0 to 10 is set: The recommended property value is 10.
•When 10 to 50 is set: The property value shall be as set.
•When 50 to 253 is set: The recommended property value is 50.

**Fig. 2.1 Property Value Setting Example 1**

(2) In a case where the number of step values that can be used for step adjustment of the operation of the actual device represented by an ECHONET property is smaller than the number of step values included in the ECHONET property definition range, and one of the values within the ECHONET property definition range that has been set in the ECHONET property is other than the step values for the actual device, it is recommended that the application software program in the ECHONET Lite node use, as the property value for the actual device and the ECHONET property value, the value that can be used for the actual device and is closest to the value previously set in the ECHONET property.

For example, when the ECHONET property definition range includes eight step values between 0x31 and 0x38 but only 0x31, 0x35 and 0x38 (three step values) can be used for step adjustment of the operation of the actual device represented by the ECHONET property, and one of the eight values within the ECHONET property definition range has been set in the ECHONET property, it is recommended that the application software program in the ECHONET Lite node use, as the property value for the actual device and the ECHONET property value, the value among the three values that is closest to the value previously set in the ECHONET property, based on mapping of the 8-value range onto the 3-value range, as shown in Fig. 2.2.

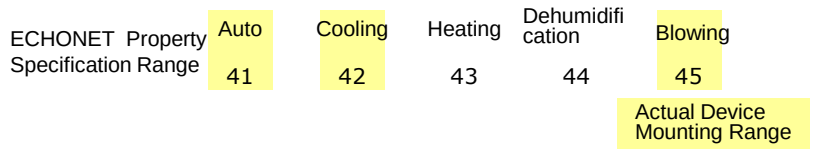



•When 31, 35, or 38 is set: The property value shall be as set.
•When 32, 33, 34, 36, or 37 is set: The property value shall be mapped close to 31, 35, or 38.

**Fig. 2.2 Property Value Setting Example 2**

(3) In a case where the previously set value in an ECHONET property specifies a function that is included in the ECHONET property definition range but is not implemented in the actual device represented by the ECHONET property, it is recommended that the application software program in the ECHONET Lite node

ignore the setting and use, as the ECHONET property value, the current value specified for the actual device, as shown in Fig. 2.3.




•When 41, 42, or 45 is set: The property value shall be as set.
•When 43 or 44 is set: The set value shall be ignored and the property value shall remain unchanged.

**Fig. 2.3 Property Value Setting Example 3**

## 2.2 Guidelines on the Handling of Responses

For a response to a property value write request (ESV=0x60, 0x61) or property value write-read request (ESV = 0x6E) of the values specified below, it is recommended to assume that the processing should have been accepted. In other words, there is no response for ESV=0x60. For ESV = 0x61, 0x6E, a property value write response (ESV = 0x71) or property value write-read response (ESV = 0x7E) is returned.

In case of an implementation that returns a response after confirming the support range of actual device or setting up actual device, a response of processing impossible (ESV=0x50, 0x51, 0x5E) may be returned.

- In a case where a value outside the ECHONET property definition range was specified.
- In a case where the continuous value range in which the actual device represented by an ECHONET property can operate is narrower than the ECHONET property definition range and a value has been set in the ECHONET property that falls between the upper and lower limit values for the ECHONET property but not between the upper and lower limit values for the actual device.
- In a case where the number of step values that can be used for step adjustment of the operation of the actual device represented by an ECHONET property is smaller than the number of step values included in the ECHONET property definition range, and one of the values within the ECHONET property definition range that has been set in the ECHONET property is other than the step values for the actual device.
- In a case where the previously set value in an ECHONET property specifies a function that is included in the ECHONET property definition range but is not implemented in the actual device represented by the ECHONET property.

## 2.3 Guidelines on OPC

A controller or similar equipment sends a property value write request (ESV = 0x60, 0x61), property value read request (ESV = 0x62), property value write-read request (ESV=0x6E), or property value notification request (ESV=0x63) to other ECHONET Lite device. If this kind of equipment receives a response of processing impossible (B smaller than A is set to OPC) to a sent request (A of 2 or greater is set to OPC), it is recommended to set B (or less) to OPC at later request send.

If the OPC processable number of the controlled equipment is unknown at this time, the possibility of receiving the expected response can be increased by setting OPC to 1 when sending the request message (ESV=0x6*).

## 2.4 Guidelines on General Broadcast

### 2.4.1 Basic Concept

Some use of general broadcasts may cause ECHONET Lite node processing overload or network congestion. The following are guidelines on sending or receiving of a general broadcast message.

- It is preferable not to send a message whose address is for a general broadcast and ESV is a property value notification request (0x63). This kind of message causes a further general broadcast because of the responses from all nodes that receive the message.
- Response concentration may be caused by messages whose addresses are for a general broadcast and ESVs are a property value write request (requiring response) (0x61), read request (0x62), notification request (0x63), or write-read request (0x6E). To ease this concentration on the sender, each node receiving this kind of message should wait for a different length of time until sending a response message. The wait time is a fixed value different for each node or is a random time.
- When using notifications or notification requests by general broadcast, applications of each node should use them without significantly impacting traffic, taking the system and communication media characteristics into account. For example, if the communication medium implements multi-hop, general broadcast of messages in large volumes can increase the network load, reducing the communication reliability of the system as a whole. Therefore, it is recommended that the transmission frequency be set in consideration of the anticipated traffic.

### 2.4.2 Concept in an IPv4 environment

If a router compatible with the “IGMP (Internet Group Management Protocol)” standard, a protocol for controlling IP multicast groups (hereinafter “multicast router”), is

on the same network, general broadcasts sent by ECHONET Lite nodes may sometimes not forwarded when the other ECHONET Lite node passing through the multicast router is not compatible with the IGMP standard. Therefore, it is recommended that ECHONET Lite nodes should be made compatible with the IGMP standard when using IPv4 to construct systems. (In particular, keep a function for sending the IGMP Membership Report when receiving Membership Queries from an IGMP Querier supporting router)

Although sending IGMP Membership Reports in the following cases is not specified in IGMP standard, it is also recommended that ECHONET Lite nodes send IGMP Membership Reports to absorb the differences in router implementation specifications and increase the success rate of multicast communications. Since the timing of deleting information from the table used to manage information required for multicast varies by router implementation specifications, sending IGMP Membership Reports in the following cases can make it more likely that information required for multicast will be in the table.

1. After obtaining a startup IP address
2. After obtaining an IP address from link-down to link-up
3. When changing IP addresses (ex. When IP address mode is changed from DHCP to Static, When DHCP lease time is expired)

Besides this, there are also multicast routers or switches equipped with an IGMP Snooping function that monitors IGMP Membership Reports and makes judgments on forwarding IP multicast packets to each port. In the case of multicast routers or switches that control the forwarding time of IP multicast packets, if the forwarding time has passed without the IGMP Membership Report being received, IP multicast packets of general broadcasts may sometimes not be forwarded to the ECHONET Lite node passing through the multicast router or switch. Therefore, it is recommended that ECHONET Lite node maintain a state that can forward general broadcasts by regularly sending Membership Reports (for example, within a 2-minute interval) to absorb the differences in router implementation specifications and increase the success rate of multicast communications.

If the ECHONET Lite node does not regularly send Membership Reports and the multicast router used does not regularly send IGMP Membership Queries, it is recommended that either another multicast router or a switch that does not have the IGMP Snooping function to control the forwarding time be selected, or that the settings of the IGMP Snooping function be changed (e.g. by disabling the forwarding time setting, turning the IGMP Snooping function OFF, etc.) when constructing the ECHONET Lite system.

Address and UDP/TCP port requirements when using IPv4 in OSI Layer 3 are defined in Section 1.2 of “Part 2 ECHONET Lite Communications Middleware Specifications”. IGMPs are specified in RFC1112 (Version 1), RFC2236 (Version 2) and RFC3376 (Version 3).

## 2.5 Guidelines on the Number of Instances

As a rule, the number of equipment object instances held by one ECHONET Lite node shall be 84 or less.

Even for a node entity having 85 or more instances, it is preferable to notify only up to 84 instances by an instance list notification (EPC = 0xD5) by considering nodes that interpret only 84 or less instances.

For the notification or interpretation of an instance list having 85 or more instances, it is preferable to use a message whose OPC value is 2 or more and each EPC value is 0xD5. However, a message sending node should note the existence of receiving nodes which do not interpret it.

## 2.6 Guidelines on the Property Value Write & Read Service

This section gives implementation guidelines for the property value write & read service.

- This service should be implemented so that a node receiving a property value write & read request (ESV = 0x6E) from another node will process the write request first, irrespective of the property combination, then store a value based on the self-node status after completion as a response to the read request. If the processing of an arbitrary property combination in this order cannot be guaranteed (write processing and equipment status change are asynchronous), the node should return a response of processing impossible (ESV = 0x5E) to a property value write & read request by setting OPCSet and OPCGet to 0.

- This service should be implemented so that, if a node sends a property value write & read request (ESV = 0x6E) to a remote node and receives a normal response (ESV = 0x7E), processing should be executed on the assumption that the write request to the remote node should have been processed and a value based on the remote node status after processing should have been acquired as a response to the read request.

## 2.7 Guidelines on Sending Messages

Many types of ECHONET Lite devices (such as equipment and sensors) have a small memory capacity and low computing power. Therefore, when sending request messages or notification messages consecutively to the same ECHONET Lite device in a short time, or when sending a new request message to the same ECHONET Lite device before the device has sent a response to an earlier one, the response from the device could be lost, or the processing relevant to each message might not be incorporated. In some ECHONET

Lite devices, messages need to be sent at intervals in the order of seconds or more. When sending messages consecutively to the same ECHONET Lite device, it is recommended that the transmission interval be designed to reflect the processing capability of different ECHONET Lite devices.

## 2.8 Guidelines on Management of ECHONET Lite Device

Two or more device objects may be mounted on the same ECHONET Lite node. In such cases, it is recommended that, when wishing to uniquely specify in units of device mounted on the same ECHONET Lite node as well as uniquely specifying the ECHONET Lite node itself, the "Identification number property (0x83)" should be implemented in the device objects and the protocol type of the lower communication layer should be 0xFE. "Identification number property (0x83)" is the number used to uniquely identify device objects within a domain. This is defined under device objects super class requirements in "APPENDIX Detailed Requirements for ECHONET Device Objects". Here, vendors have to ensure that the unique ID fields of "identification number property (0x83)" are not overlapping within the same class for a manufacturer's specific code (0xFE) .

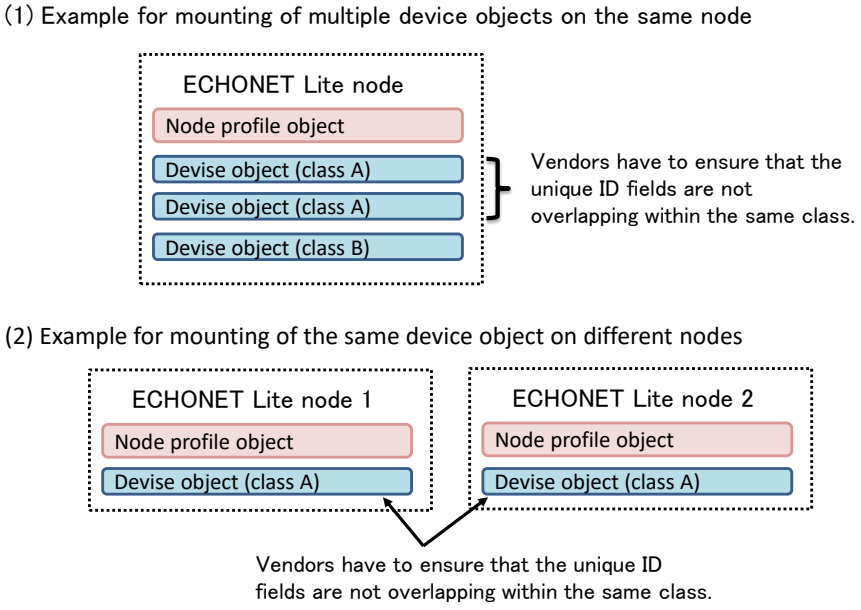



**Fig. 2.4 Device object and identification number property**

## 2.9 Guidelines on Implementation of ECHONET Properties

This section gives guidelines on the implementation of ECHONET properties.

### 2.9.1 Concept of objects implemented in ECHONET Lite middleware adapters

When connecting to the ECHONET Lite network with a combination of ECHONET Lite-ready equipment and ECHONET Lite middleware adapter, device object properties show information related to ECHONET Lite-ready equipment, while node profile object properties show information related to the ECHONET Lite middleware adapter.

For example, device object properties such as the serial number, product code, and manufacturer code show information related to ECHONET Lite-ready equipment, while node profile object properties such as the serial number, product code and manufacturer code show information related to the ECHONET Lite middleware adapter.

### 2.9.2 Concept of implementing operation status properties

For such nodes that have device objects for multiple classes, the “Operation status property (0x80)” can be implemented with the fixed value of 0x30 only when the functions specific to the corresponding classes starts to work in accordance with the beginning of the node operation. In this case, it is recommended that the access rule is limited to “Get” only. The “Operation status property (0x80)” indicates whether or not the functions specific to each class in actual device are in operation status (ON/OFF), and is defined under Device Object Super Class Requirements in “APPENDIX Detailed Requirements for ECHONET Device Objects”.

### 2.9.3 Concept of implementation of manufacturer code properties

Devices that have acquired ECHONET Lite certification and AIF certification must implement manufacturer codes used for the application of these certifications as manufacturer codes for device objects. If the manufacturer codes are changed to codes that were not used to apply for certification, the device must be recertified.

## 2.10 Guidelines on Handling Transmission-only Devices

ECHONET Lite defines transmission-only devices to make not only always-live

communication devices but also battery-driven devices of low power consumption compatible with ECHONET Lite. Guidelines are available on the handling of these special devices.

- When a transmission-only device joins a network, other devices that are not transmission-only in the system shall be set manually to recognize the transmission-only device.
- When a controller joins a system that has a transmission-only device, information of the transmission-only device shall be set manually in the controller.
- It is recommended that transmission-only devices should periodically broadcast the instance list notification announcement described in Section 4.3.1 of Part II.

## 2.11 Guidelines on TCP

- The behavior of a node sending a response message to another node shall be implementation-dependent (no response necessary) if the connection is already cleared at send processing.

- A node sending a request message to another node should send the message again by UDP unicast when necessary in case of a TCP connection failure since the remote party may not be able to use TCP.

## 2.12 Cautions regarding wireless LAN networks

There are routers and relays that regularly update group keys to be used for multicast communication and increase communication safety. Requirements to update group keys are not specified in standard specifications such as 802.11i; therefore, router and relays are implementation-dependent. Therefore, when such routers and relays exist on the same network, group keys are often inconsistent among ECHONET Lite nodes. It is therefore recommended that the ECHONET Lite node implement wireless LAN to detect group key updates and re-acquire group keys.

For example, group key updates can be monitored by regularly sending DHCP requests that set the broadcast flag to True (see RFC2131) from the ECHONET Lite node to a router (e.g. Discover and T2 Request). New group keys can be obtained by executing a 4-way handshake after reestablishing a wireless connection; this is done by deeming that the group key has been updated when a broadcast response from router (e.g. Offer and Ack) can no longer be received. Group key inconsistency can also be solved by executing a 4-way handshake after manually reestablishing a wireless connection; this is done by indicating a message to urge users to reboot the ECHONET Lite node, router, and relay on the UI.

Additionally, group key inconsistency can be resolved by changing the update interval of either the router or replay (e.g. to 10 minutes).

# Chapter 3 Guidelines for Secure Communications in ECHONET Lite

## 3.1 Overview

For secure communications in ECHONET Lite, tampering with communications is prevented: illegal access is prevented by authentication, and tapping is prevented by encryption. The ECHONET Lite Communication Middleware ensures security transmissively from ECHONET Lite by applying the existing standard technologies for secure communications to its lower layers. This chapter gives examples of mechanisms for secure communications in lower layers and describes their guidelines.

## 3.2 Secure Communications in Lower Layers

This section gives examples of mechanisms for secure communications in lower layers that are provided by the ECHONET Lite Communication Middleware. Security may also be ensured by using not the following mechanisms but the unique mechanism of each company. Negotiation by encryption algorithms, the encryption of communications between ECHONET Lite nodes, and authentication between ECHONET Lite nodes shall follow the specifications of each secure communications mechanism.

**Table 3.1 Mechanisms for Secure Communications in Lower Layers**

| Lower Layer | Mechanism for Secure Communications |
|---|---|
| Transport | DTLS (Datagram Transport Layer Security) |
| Network | IPsec (Security Architecture for Internet Protocol)<br>RFC5191 |
| Data Link | WEP (Wired Equivalent Privacy)<br>WPA (Wi-Fi Protected Access)<br>WPA2 (Wi-Fi Protected Access2)<br>AES-CCM (Advanced Encryption Standard Counter with CBC-MAC)<br>IEEE802.1X |

### 3.2.1 DTLS

DTLS is a protocol to provide secure communication functions for datagram. The functions are almost the same as those of TLS (Transport Layer Security). The use of DTLS on a UDP is specified in RFC4347. This protocol is applicable when using UDF in the transport layer or when encrypting ECHONET Lite transmission frames and preventing tampering in the transport layer.

### 3.2.2 IPsec

IPsec is a protocol to provide functions for keeping data confidential and preventing tampering in units of an IP packet. This protocol is an option for IPv4 but is implemented in IPv6 as a standard feature. This protocol is applicable when using IP in the network layer or when encrypting ECHONET Lite transmission frames and preventing tampering in the network layer.

### 3.2.3 RFC5191

RFC5191 is a standard to regulate connections by authentication so that only specified devices can join a network. This standard is available in an arbitrary data link layer. A recommended configuration is where an ECHONET Lite node serves as a client issuing an authentication request and a device capable of communicating with an ECHONET Lite node serves as an authentication agent or server receiving an authentication request. A recommended authentication system is PEAP for authentication with an ID or password using a serial key marked on the frame of a device or EAP-TLS for authentication with a digital certificate stored in a device.

### 3.2.4 AES-CCM

The next-generation encryption system of the U.S. Government established by the National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce. Counter Mode is used for encryption, Message Integrity Code (MIC) for detecting and preventing tampering, and CBC-MAC for MIC generation.

### 3.2.5 WEP

An encryption technology for wireless communications. This secret key encryption system, based on the RC4 algorithm, is standardized by IEEE and adopted as a security system of IEEE 802.11b.

### 3.2.6 WPA

A standard of encryption system for wireless LAN announced by the Wi-Fi Alliance, which is an organization in the wireless LAN industry. The security strength of WEP was improved by compensating for its vulnerable points. For encryption, WPA has a user authentication function, as well as SSID and WEP key, and uses the Temporal Key Integrity Protocol (TTKIP)), which updates the encryption key automatically at fixed time intervals.

### 3.2.7 WPA2

A new version of WPA. This system uses the encryption standard AES specified by the U.S. National Institute of Information and Communications Technology (NICT) for powerful encryption using keys of variable length from 128 to 256 bits.

### 3.2.8 IEEE802.1X

IEEE802.1X is a standard to regulate connections by authentication so that only specified devices can join a network. This standard is available both for cable and wireless communications. A recommended configuration is where an ECHONET Lite node serves as a supplicant (authentication client) and a device capable of communicating with an ECHONET Lite node serves as an authenticator (authentication device) or authentication server (server which judges whether to allow a supplicant to participate). A recommended authentication system is PEAP for authentication with an ID or password using a serial key marked on the frame of a device or EAP-TLS for authentication with a digital certificate stored in a device.

# Chapter 4 Guidelines on Node Detection and Finding Procedure

## 4.1 Concept

Except for regular communications with fixed parties, an ECHONET Lite node to control other ECHONET Lite nodes or acquire their statuses (hereinafter, referred to as “controller” in this chapter) acquires communications addresses by node detection and finding before starting communications.

ECHONET Lite does not define a node detection or finding message. However, this can be realized by combining a general broadcast and the acquisition and notification of essential properties to be mounted. This chapter gives guidelines on the procedure.

## 4.2 Detection by Message Send from Node to Controller

When joining a network (including a change of communication address), an ECHONET Lite node must send an instance list notification message by a general broadcast according to "Part II 4.3.1 Basic Sequence for ECHONET Lite Node Startup." To detect the joining of a new node immediately, the controller may wait for and process the message.

If all nodes start simultaneously after recovery from a power failure, simultaneous transmission may cause network congestion. To ease this congestion, each node should wait for a different length of time after newly joining a network until sending an instance list notification message. The wait time is a fixed value different for each node or is a random time.

## 4.3 Finding by Message Send from Controller to Node

To find ECHONET Lite nodes within the network, a controller may send a node finding message by a general broadcast at an arbitrary timing. All ECHONET Lite nodes wait for the message, except transmission-only devices. A node must return a response if the message is related to its own object or property. For a node finding message, it is preferable to use the following parameters:

- Destination address: General broadcast
- TID: Arbitrary value
- SEOJ: One of the objects held by the controller
- DEOJ: Node profile object (0x0EF001)
- ESV: Property value read request (0x62)
- OPC: 1

- EPC: Self-node instance list S (0xD6)

To find a specific model (node having specific equipment objects), the following parameters may be used:

- Destination address: General broadcast
- TID: Arbitrary value
- SEOJ: One of the objects held by the controller
- DEOJ: Equipment object held by a node to find
- ESV: Property value read request (0x62)
- OPC: 1
- EPC: Properties held by DEOJ-specified objects (preferable to specify the operation status (EPC = 0x80) and other essential properties)

It is preferable not to use a property value notification request (0x63) for ESV of a node finding message. A message whose destination is an address for a general broadcast and ESV is a property value notification request causes a further general broadcast because of the responses from all nodes that receive the message. This may result in node processing overload or network congestion. Therefore, the controller waits for a certain time after sending the node finding message. The wait time may be a fixed value or a variable value depending on the network status.

## 4.4 Confirmation of ECHONET Lite Device Connections

The ECHONET Lite Specification contains no provisions for device to notify other nodes that they are still connected to the network. However, some ECHONET Lite nodes periodically transmit instance list notification messages to notify that they are connected to the network, as in the case of transmission-only devices. It is recommended that ECHONET Lite device, on receiving a message, should judge whether or not the transmitting equipment needs to be newly registered, and divide the processing accordingly. It is also recommended that the transmission interval design of equipment that transmits instance list notification messages should take into account the fact that some receiving equipment processes registration of new equipment.

# Chapter 5 Guidelines on Remote Control

## 5.1 Basic Concept

In this section, nodes that transmit control request messages (ESV=0x60, 0x61, 0x62, 0x63, 0x6E) shall be defined as “controllers” and those that receive control request messages as “devices”. The purpose of the remote control setting property (0x93) provided from APPENDIX Release C or later is to enable “devices” to distinguish whether they are controlled through a public network.
An additional definition is that it can be obtained from the controller whether a given device is in

- a state in which it recognizes to be controlled through a public network (0x42)
- a state in which it recognizes to be controlled through other way but a public network (0x41).

It is recommended that controllers that control through a public network and devices that are controlled through a public network (devices recognized to be controlled and operated through a public network) should implement the “remote control setting property (0x93)”.

However, in systems compatible with ECHONET device objects up to APPENDIX Release B or earlier, it is not possible to distinguish or judge whether devices are controlled through a public network or not. Even APPENDIX Release C or later, the same is true of systems containing controllers that do not implement the function of transmitting control request messages which attached the remote control setting property (0x93).

In such systems that cannot distinguish whether devices are controlled through a public network or not, it is recommended, erring on the side of caution, that devices should be operated as if they were fully controlled through a public network.

## 5.2 When Using Middleware Adaptors

Guidelines when using object generation type middleware adapters and ready devices to implement remote control will be given here.

APPENDIX Release C stipulates that, for control through a public network, several properties including the remote control setting property shall be stored in one message and the message sent as a control request. When the message is sent, the remote control setting property shall always be attached to the first property and transmitted as EDT=0x42 (operation through a public network). Meanwhile, when not controlling through a public network, the rule is that a control request message shall be sent without giving the remote control setting property.

Below, two methods are indicated for a middleware adapter that has received this control request message to transmit the content of the message to a device. It is recommended that middleware adapters and ready devices capable of remote control should be equipped with one of these methods.

In either case, the access rules of the remote control setting property shall be IASetup and IAGetup. Similarly, the access rules shall also be IASetup and IAGetup for properties when wanting to distinguish between control sources through a public network and those not through a public network.

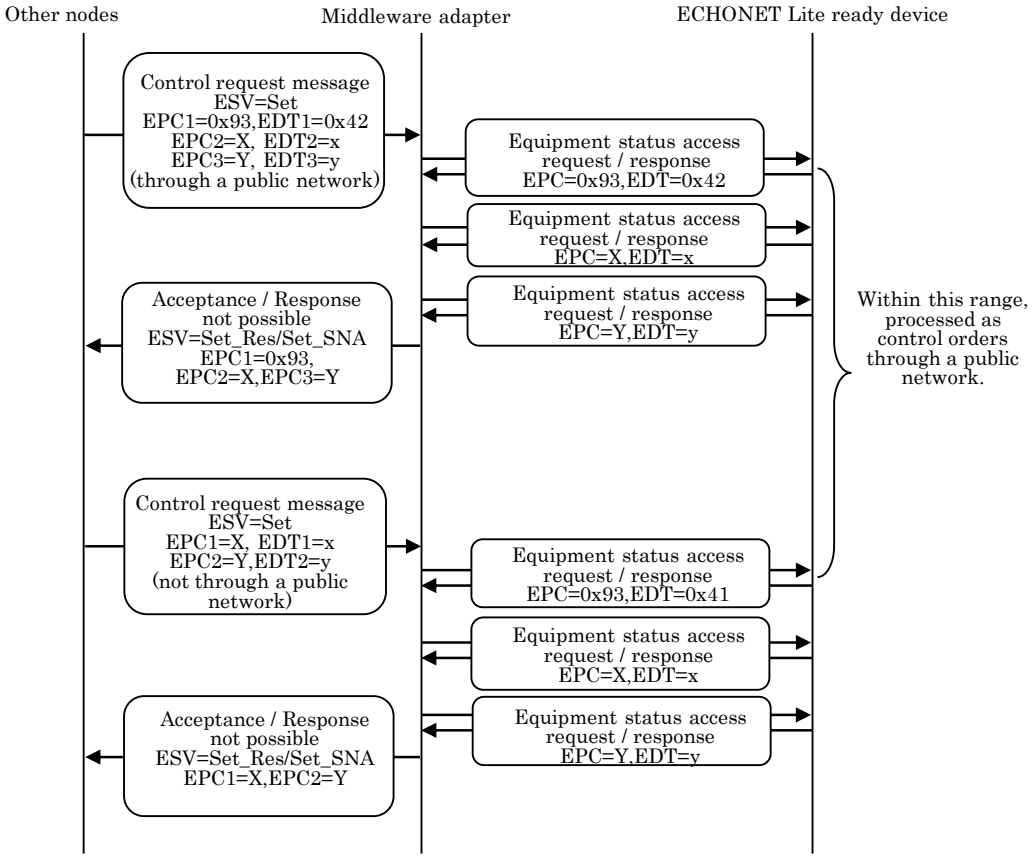
(1) Method using “equipment status access request / response commands”

When a control request message has been received through a public network, the middleware adapter shall follow the process in 3.8.5.8 of Part 3. When doing so, equipment status access request and response commands shall be used.

When receiving a control request message not through a public network, if the previous control request message was received through a public network, the middleware adapter uses an equipment status access request to forward the remote control setting property (0x93) as EPC and control not through a public network (0x41) as EDT to ready devices. The response to the remote control setting property received from ready devices is discarded and is not included in the final response to the control request message. After this, the process follows 3.8.5.8 of Part 3.

The purpose of this process is to enable recognition of the boundary between commands to ready devices through a public network and those to devices not through a public network.

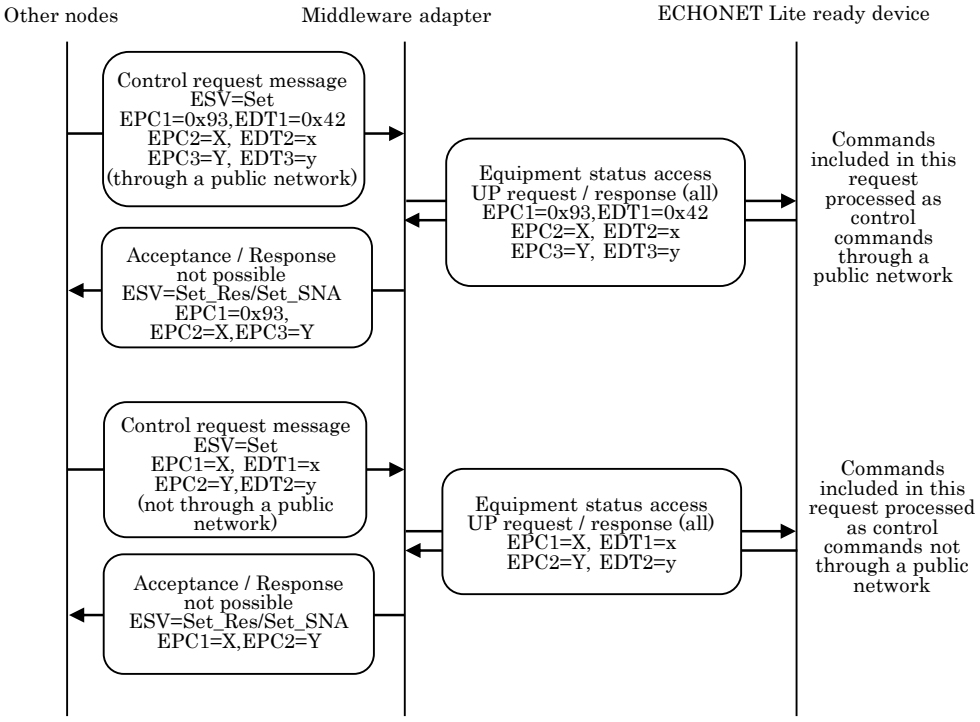
Ready devices process as a control order through a public network once they have received the request to set the remote control setting property (EPC=0x93) in control through a public network (EDT=0x42). After receiving a request to set the remote control setting property (EPC=0x93) in control not through a public network (EDT=0x41), they process as a control command not through a public network. This is illustrated in the diagram below.




While the above control request message is being processed, i.e. in the time from when the middleware adapter receives the control request message and forwards the first equipment status access request to ready devices until the final equipment status access response is received from ready devices, the middleware adapter shall use some mechanism of exclusive control to prevent interruption by other equipment status access requests and equipment status access UP request (all) commands.

(2) Method using “equipment status access UP request / response (all)” commands
The middleware adapter follows 3.8.5.8 of Part 3. When doing so, “equipment status access UP request / response (all) commands” are used.

After receiving an equipment status access UP request (all), ready devices process it as control through a public network if the request includes a request to set the remote control setting property (EPC=0x93) in control through a public network (EDT=0x42). If not included, it is processed as control not through a public network. This is illustrated in the diagram below.



# Chapter 6 Implementation Cases and Policies on Smart Electric Energy Meters

This chapter gives implementation cases where there were problems with interoperability and expected actions related to the Application Communication Interface Specifications between Low-voltage Smart Electric Energy Meters and HEMS Controllers [LSM_AIF] and the Application Communication Interface Specifications between High-voltage Smart Electric Energy Meters and HEMS Controllers [HSM_AIF].

## 6.1 Implementation cases for simplex meters

(1) Target devices

Low-voltage smart electric energy meters

(2) Cases

For low-voltage smart electric energy meters, when combining a communication unit designed to be combined with a duplex measuring section and simplex measuring section, it may violate [LSM_AIF] specifications. The duplex measuring section measures the electric energy in both the normal and reverse directions, while the simplex measuring section measures electric energy in only the normal direction.

Implementation case that violates specifications:

For low-voltage smart electric energy meters, when combining a communication unit designed to be combined with a duplex measuring section with a simplex measuring section, the communication unit sends "0x00000000" as a cumulative value property (reverse direction).

(3) Expected actions

1) If there is non-compliance with the combination specifications of the communication unit and the measuring section, corrections must be made at the earliest possible stage. Note that if problems are found in products sold in the market, certification may be canceled.
2) Check whether measuring section to be combined with the communication unit is a simplex measuring section or duplex measuring section. If the communication unit is made for a simplex measuring section, the following correspondences must be taken.
   - If combining the communication unit with the measuring section in the simplex direction, indicate that the meter is a simplex meter by excluding reverse direction properties from the property map.
   - If including reverse direction properties in the property map by combining the communication unit with a measuring section for the simplex direction, always send "0xFFFFFFFE" (no measured data) when sending a Get response.

## 6.2 Implementation cases for "Day for which the historical data of measured cumulative amounts of electric energy is to be retrieved" property

(1) Target devices

Low/high-voltage smart electric energy meters

(2) Cases

It has been confirmed that in some smart electric energy meters the value set in the "Day for which the historical data of measured cumulative amounts of electric energy is to be retrieved" property is not immediately reflected in the value of the "Day for which the historical data of measured cumulative amounts of electric energy is to be retrieved 1" property acquired. For example, there are cases where historical data from a day other than the set retrieval day is sent, which happens when a communication failure in route B occurs between setting the retrieval day property and acquiring the retrieval day 1 property. If setting the date that a power failure occurs to "Day for which the historical data of measured cumulative amounts of electric energy is to be a retrieved" property, there are some cases where "the day for which the historical data of measured cumulative amounts of electric energy to be retrieved", which is represented with the first two bytes of the obtained "Historical data of measured cumulative amounts of electric energy 1" property, is set to "undetermined" (0x00FF).

(3) Expected actions

For smart electric energy meters, regardless of conditions such as re-connection, the first two bytes of the "Day for which the historical data of measured cumulative amounts of electric energy is to be retrieved 1" property (EPC=0xE2 and 0xE4) must be same as the value set for the "Day for which the historical data of measured cumulative amounts of electric energy is to be retrieved" property (EPC=0xE5).

## 6.3 Implementation cases for cumulative electric energy value when lacking measured data

(1) Target devices

Low/high-voltage smart electric energy meters

(2) Cases

When no electric energy measured data exists because the measurement of electric energy failed due to a power failure or other event, the measured cumulative amount of electric energy of cumulative value historical data (or cumulative value of the latest time) property must be 0xFFFFFFFE (no measured data). However, there are some cases where smart electric energy meters violate [LSM_AIF] specifications when there is no measurement data, having 0x00000000 as a measured cumulative amount of electric energy.

Related EPC (property name)

Historical data:

0x E2 (Historical data of measured cumulative amounts of electric energy 1 (normal direction))

0x E4 (Historical data of measured cumulative amounts of electric energy 1 (reverse direction))

0x E5 (Day for which the historical data of measured cumulative amounts of electric energy is to be retrieved 1)

0x EC (Historical data of measured cumulative amounts of electric energy 2 (normal and reverse directions))

0x ED (Day for which the historical data of measured cumulative amounts of electric energy is to be retrieved 2)

Current data:

0x E0 (Measured cumulative amount of electric energy (normal direction))

0x E3 (Measured cumulative amount of electric energy (reverse direction))

0x EA (Cumulative amounts of electric energy measured at a fixed time (normal direction))

0x EB (Cumulative amounts of electric energy measured at a fixed time (reverse direction))

(3) Expected actions

If there are no time data of electric energy measured data due to data not measured or outside the historical data retention period (data deletion) or other event, the measured cumulative amount of electric energy must be "0xFFFFFFFE (no measured data)" should be the proper value, instead of "0x00000000". Note that if the violation of [LSM_AIF] specifications is found on the products sold in market, the certification may be canceled.

## 6.4 Implementation cases on living confirmation method

(1) Target devices

Low/high-voltage smart electric energy meters and HEMS/EMS controllers

(2) Cases

The ECHONET Lite specifications specify not for the sequence of "living confirmation (Keep Alive)" that periodically check if the connection is kept with the counterpart. For this reason, a variety of implementations are mixed, and this may cause problems in terms of interoperability.

So far, the following implementations were reported.

1) Neighbor Solicitation—Advertisement of IPv6 layer
2) Enhanced Beacon Request—Enhanced Beacon of MAC layer (802.15.4e) of Wi-SUN
3) SetC/Get command—Set_Res/Get_Res of ECHONET Lite layer
4) Echo Request—Echo of ICMPv6 (not ideal, since it can be disabled)

5) Simple Service Discovery Protocol (SSDP) UD for Universal Plug and Play (UPnP)P Port = 1900 (not ideal, since it is uncommon to be implemented for route B)

[Supplemental information] PANA Notification Request (AUTH, P-bit): As a part of the PANA Authentication, communication for living confirmation (Section TR-1052 2.8.3.1.2) is specified.

(3) Expected actions

In general, "living confirmation" is carried out using required functions. For low-voltage smart electric energy meters, it is preferable to use the required functions of Wi-SUN or ECHONET Lite. For high-voltage smart electric energy meters, it is preferable to use the required functions of ECHONET Lite.

## 6.5 Implementation case for reconnection attempt

(1) Target devices

HEMS controller

(2) Cases

Some low-voltage smart electric energy meters implement a function that stops route B ECHONET Lite communication when the specified time comes daily, regardless of the Session Life Time of the PANA authentication. In this regard, it has been confirmed that low-voltage smart electric energy meters respond to communication of the lower layers such as MAC layer and IPv6 layer, but do not respond to PANA and ECHONET Lite communication.

When failing to verify whether the low-voltage smart electric energy meter is alive or unable to maintain ECHONET Lite communication, if a HEMS controller starts over from “Active Scan”, it takes too long to re-establish a connection. Some data loss cases while waiting for the reconnection have been reported.

(3) Expected actions

Based on the cases described above, the HEMS controllers should be designed considering the disengagement of low-voltage smart electric energy meters. A HEMS controller should reconnect to a low-voltage smart electric energy meter when the HEMS controller cannot confirm that the meter is alive. It is expected that the reconnection procedure will start from one of the following stages. However, as it goes from 1) to 4), the time required to establish reconnection increases.

1) PANA re-certification
2) PANA first-time certification
3) Enhanced Beacon Request
4) Active Scan for all Channels

[Supplemental information] For more details on reconnection, see the descriptions in “TTC TR-1052

HEMS—Detailed implementation guideline for communication interface between HEMS and Smart meter (Route-B)

## 6.6 Implementation case for starting ECHONET Lite communication

(1) Target devices

Low-voltage smart electric energy meters and HEMS controllers

(2) Cases

The [LSM_AIF] shows an example of an ECHONET Lite communication starting sequence after completion of PANA authentication. If a device expects the counterpart to always follow the example sequence exactly and does not accept other sequences, it cannot communicate with ECHONET Lite even after PANA authentication succeeds.

So far, the following implementations have been reported.

- The ECHONET Lite communication cannot be started unless receiving a startup INF (EPC=0xD5) from the counterpart. Therefore, ECHONET Lite communication cannot start if there is a failure to receive a startup INF for some reason.
- The shift in timing for receiving startup communications from the counterpart is not tolerated, so ECHONET Lite communication cannot start if the sending/receiving timing is shifted.
- When the HEMS controller sends INF_Req immediately after the completion of PANA authentication, ECHONET Lite communication will not start, because smart electric energy meters cannot complete preparations to receive messages in time.
- Some low-voltage smart electric energy meters only send startup INF when establishing a route B connection for the first time after power-on.

(3) Expected actions

- After the completion of PANA authentication, the respective HEMS controllers and smart electric energy meters immediately start communication as ECHONET Lite nodes and send instance list notifications. The HEMS controller in particular should not use the receipt of the instance list notification sent from the smart electric energy meters as a trigger to start ECHONET Lite communication of their own devices.
- After completion of PANA authentication, if the HEMS controllers for low-voltage smart electric energy meters fail to receive an instance list even after waiting for a while, it is recommended under [LSM_AIF] specifications to obtain the instance list notification of the counterpart using unicast INF_Req[0x63].
- It should be taken into account by implementations that the processing performance of the counterpart can be different from that of themselves. Note especially that HEMS controllers should allow enough margin for receiving timing and transmit intervals in consideration of the fact that the processing performance of smart electric energy meters (not limited to communication processing) can be very low.

## 6.7 Implementation case for replacing controllers

(1) Target devices

Low/high-voltage smart electric energy meters and HEMS/EMS controllers

(2) Cases

If any restrictions or procedures are required for smart electric energy meters when replacing old HEMS/EMS controllers with new ones, it may cause users needless confusion.

Cases where the smart electric energy meter requires restrictions or procedures:

1) Cases where once the route B connection is established, the smart electric energy meter fails to connect to new HEMS controllers, unless the disconnecting procedure is taken. (General users often disengage old HEMS controllers without going through the proper disconnecting procedure, so they have problems connecting to new HEMS controllers.)
2) Cases where new HEMS controllers cannot be connected without disconnecting the primary power source at the side of smart electric energy meters for at least 10 seconds. (This is virtually impossible, since the main power supply must be cut off.)
3) Cases where once route B is disconnected, the smart electric energy meter fails to connect to new HEMS controllers, unless at least 24 hours have elapsed. (This means that users cannot know when they can connect to new HEMS controllers.)

(3) Expected actions

Note the smart electric energy meter should avoid cases 1) and 2) above.

Also, it is considered inappropriate to create a time window where connection requests cannot be accepted (see cases 3) above, as connection requests must always be accepted under normal operation.

However, if multiple controllers exist in same network domain, there are concerns that two or more controllers may compete with each other to connect to one smart electric energy meter alternately. Therefore, it is preferable to establish a controller mechanism to avoid a situation where two or more controllers are competing to secure smart electric energy meters alternately when multiple controllers exist (for example, allowing inactivation of the auto connection function).

## 6.8 Implementation case on how to respond to historical data on cumulative amounts of electric energy before establishing a route B connection

(1) Target devices

Low/high-voltage smart electric energy meters

(2) Cases

There are some smart electric energy meters that configure a route B connection through route A.

They can be categorized into two types: (1) those that can send historical data on cumulative amounts of electric energy before establishing a route B connection; and (2) those unable to send the same. It has been reported that the smart electric energy meters described in (2) above can be further be categorized into two types: (1) those that respond to a Get command with 0xFFFFFFFE (no measured data) and; (2) those respond with Get_SNA.

(3) Expected actions

For smart electric energy meters that are unable to send historical data on cumulative amounts of electric energy before a route B connection is established, it is preferable to respond with 0xFFFFFFFE (no measured data) for the Get command. Responding with Get_SNA does not violate [LSM_AIF]/[HSM_AIF] specifications, but still, manufacture vendors should take care to make sure that Get commands may be repeatedly sent.

## 6.9 Implementation case on abnormalities during PANA authentication

(1) Target devices

Low-voltage smart electric energy meters and HEMS controllers

(2) Cases

There are some cases where route B communication at low-voltage smart electric energy meters is disconnected when an unexpected PANA packet is received from HEMS controllers during the PANA authentication sequence.

There are some cases where a communication module at a Low-voltage smart electric energy eeter stops its operation if it receives an error notification sent from a HEMS controller during PANA authentication.

(3) Expected actions

When an authentication error is detected during the PANA authentication, it is preferable that the HEMS controller and the low-voltage smart electric energy meters should respectively perform actions that comply with the description in TTC TR-1052. Further, low-voltage smart electric energy meters should restart PANA authentication after disregarding it instead of stopping its operation, even if an unexpected PANA packet is received.

## 6.10 Implementation case for measured cumulative amount of electric energy

(1) Target devices

Low/high-voltage smart electric energy meters

(2) Cases

There are some meters that only update measured cumulative amount of electric energy (EPC=0xE0, 0xE3) values every 30 minutes and the values are consistent with those of cumulative

amounts of electric energy measured at a fixed time (EPC=0xEA, 0xEB). Because current values cannot be obtained, precise control of demand and response becomes difficult.

(3) Expected actions

Smart electric energy meters should send current values as values for EPC=0xE0 and 0xE3.

## 6.11 Implementation case for taking measures against DOS attack (1)

(1) Target devices

Low/high-voltage smart electric energy meters and HEMS/EMS controllers

(2) Cases

It has been confirmed that some smart electric energy meters become unable to communicate for 10 minutes if they receive 60 or more times per minute, as a measure against DOS attack (Denial of Services). There are cases where similar symptoms are presented; not only for ECHONET Lite commands, but also for communication with HEMS/EMS controllers that frequently use IPv6 commands such as "Neighbor Solicitation".

(3) Expected actions

For smart electric energy meters, it is preferable to implement functions that do not have excess restrictions on operation as described above.

For HEMS/EMS controllers, it is essential to assume that there will be cases involving the behaviors described above, to allow access to smart electric energy meters at a sufficient interval for cases where a normal connection has been established, in consideration of lower layer communications such as "Neighbor Solicitation". If there is no data response, appropriate recovery procedures should be taken (e.g. Waiting for the interval based on AIF certification, retransmission complies with lower layer communication specifications, and reconnection when not being able to communicate for a while).

## 6.12 Implementation case on taking measures against DOS attack (2)

(1) Target devices

Low-voltage smart electric energy meters

(2) Cases

The following DOS attack may be established, if the low-voltage smart electric energy meter can switch the connection from the HEMS controller to newly connected one, when a HEMS controller tries to connect a low-voltage smart electric energy meter through route B with Wi-SUN.

When the low-voltage smart electric energy meter receives an Enhanced Beacon Request (EBR) from a new HEMS controller and releases the connection of the currently connected HEMS controller, malicious attackers can disturb communication between HEMS controllers and low-voltage smart

electric energy meters by sending EBR.

(3) Expected actions

It is preferable for low-voltage smart electric energy meters to keep the connection of the connected HEMS controller and not release the existing connection at the time of EBR reception until the PANA authentication of the HEMS controller requesting new connection is completed.