|  |  |
| --- | --- |
| Project | **IEEE 802.21.1 Media Independent Services** **<**[**http://www.ieee802.org/21/**](http://www.ieee802.org/21/)**>** |
| Title | **HEMS use case proposal for IEEE802.21.1 draft standard** |
| DCN | **21-15-0079-03-SAUC** |
| Date Submitted | **Octber 27th, 2015** |
| Source(s) | Yusuke Shimizu (Panasonic), Yuji Unagami (Panasonic) |
| Re: | IEEE 802.21.1 Plenary meeting |
| Abstract | This document describes the use case for applying IEEE802.21 to HEMS(Home Energy Management System).Home Gateway(HGW) as PoS with GM sends control command to each device as PoS and controls it.  |
| Purpose | To propose the use case for applying IEEE802.21 to HEMS. |
| Notice | This document has been prepared to assist the IEEE 802.21 Working Group. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release | The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE’s name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE’s sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that IEEE 802.21 may make this contribution public. |
| Patent Policy | The contributor is familiar with IEEE patent policy, as stated in [Section 6 of the IEEE-SA Standards Board bylaws](http://standards.ieee.org/guides/opman/sect6.html#6.3) <[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://127.0.0.1:4664/cache?event_id=757737&schema_id=1&s=5X0vID10lu_E6yrIkWkNd4Wz2H8&q=hancock)> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/faq.pdf> |

**Table of Contents**

[1.1 HEMS use case 3](#_Toc431971035)

[1.1.1 Introduction 3](#_Toc431971036)

[1.1.2 Service scenarios and call flows 4](#_Toc431971037)

[1.1.3 CRL 11](#_Toc431971038)

[1.1.3.1 CRL operation 11](#_Toc431971039)

[1.1.3.2 CRL format 12](#_Toc431971040)

[1.1.3.3 Distribution of CRL 12](#_Toc431971041)

[1.1.3.4 Size of CRL 13](#_Toc431971042)

* 1. HEMS use case
		1. Introduction

　This sub-clause explains general overview of the HEMS(Home Energy Management System) use case.

HEMS is the system to manage the energy usage in home.　HEMS with connecting devices (i.e. home appliances or equipments) realizes the "visualization" of electricity or gas consumption and the "auto control" of devices.

　HEMS typically includes Home Gateway(HGW) and the various devices as follows;

　・Air conditioning system

　・Lighting

　・Smart meter

　・PV(Photovoltaics)

　・Home security

HGW and devices are connected in home by wired or wireless network. HGW controls home appliances and collects usage information through the network.

For example, user operates HGW, and HGW can execute the collective lightings power off and the centralized control of the air conditioning system. Moreover, devices send usage state of electricity to HGW, and HGW displays the amounts of electric energy in home.

Figure 1 shows structure example of HEMS. HGW connects to devices such as PV, Air conditioning system, and lighting devices by home area network. In this example, HGW and terminal devices are connected via the cloud server, and user can control HGW by using the terminal device. HGW may collectively send a control message to the devices using a multicast transport, and the devices sends usage information to HGW in response to the control message. In this use case, Media independent service framework (MIS) of IEEE802.21 specifications is applied to the Interface between the HGW and the devices. HEMS performs the collective control of the devices and the acquisition of usage information. The controlling system of HGW by using the terminal devices via cloud server(dotted line in Figure.1) is out of scope of this use case.



Figure 1— Structure example of HEMS

* + 1. Service scenarios and call flows

This sub-clause describes the service scenario and IEEE 802.21 call flows.

Figure 2 shows the 802.21 system architecture in corresponding to HEMS structure and Figure 3, 4, and 5 shows the command flows corresponding to the different types of communication.

In this case, HGW as “PoS with GM” operates the connecting devices as “PoS”. HGW controls the power switch or settings of devices and collects the state of them. HGW operates Multicast Group Management described in IEEE 802.21.m as PoS with GM.

PoS with GM transmits control commands to PoSes and controls them. When the PoS with GM collectively controls PoSes, it sends the control command by a multicast transport. PoS sends usage information regularly to the PoS with GM. And PoS, when receiving the acquisition command of the usage information from the PoS with GM, sends the usage information of the device to the PoS with GM.



Figure 2—System architecture in 802.21

 Table 1 shows the list of Service management primitives used in HEMS use case. MIH\_LINK\_SAPs used in Link layer are not required, since the control command transmission and the usage information acquisition in HEMS are independent of the media.

Table 1— Service management primitives for HEMS use case

|  |  |  |
| --- | --- | --- |
| Service management primitive | Comments | Defined in |
| MIH\_ Configuration\_Update | This command is sent by a PoS to a group of other PoS(es) to update their configuration.In the use case of HEMS, PoS sends the HEMS control command and the usage information. | 7.4.34 |
| MIH\_Net\_Group\_Manipulate | This command is sent by a PoS to a group of other PoS(es) to create, delete or update a group membership. | 7.4.36 |
| MIH\_Push\_Certificate | This command is sent by a PoS to another PoS or an MN and it is used for sending of a certificate. | 7.4.38 |
| MIH\_Revoke\_Certificate | This command is sent by a PoS to a group of PoS(es) and/or an MN to revoke a certificate previously issued by the PoS. | 7.4.39 |

Figure 3 shows the control command flow from PoS with GM to each PoS and Figure 4 shows the notification command flow from each PoS to PoS with GM.

In Figure3, PoS with GM sends control commands to each PoS. Cipher communication of control commands uses MIH\_Configuration\_Update. Multicast cipher communication from PoS with GM to each PoS uses the MIH protocol protection.



Figure 3—Transmission of the control command

1. MIH User of PoS with GM generates the HEMS control commands for PoS, and sends it to the local MIHF using the MIH\_Configuration\_Update.request primitive.
2. MIHF of PoS with GM sends the HEMS control commands for PoS using the MIH\_Configuration\_Update indication message.
3. MIHF of PoS receives the MIH\_Configuration\_Update indication message, and sends it to the MIH User using the MIH\_Configuration\_Update.indication primitive.
4. MIH User of PoS receives the MIH\_Configuration\_Update.indication primitive, and runs the control command.

In Figure 4, each PoS notify their usage state information to PoS with GM



Figure 4—Transmission of the usage information

1. MIH User of PoS generates the usage information, and sends it to the local MIHF using the MIH\_Configuration\_Update.request primitive.
2. MIHF of PoS sends the usage information to the PoS with GM using MIH\_Configuration\_Update indication message.
3. MIHF of PoS with GM receives the MIH\_Configuration\_Update indication message, and sends it to the MIH User of PoS with GM using the MIH\_Configuration\_Update indication primitive.
4. MIH User of PoS with GM receives MIH\_Configuration\_Update.indication primitive, and collects the usage information.

In Figure 5, PoS with GM sends group membership to each PoS



Figure 5—Transmission of group membership

1. MIH User of PoS with GM generates group membership for PoS, and sends it to the local MIHF using the MIH\_Net\_Group\_Manipulate.request primitive.
2. MIHF of PoS with GM sends group membership for PoS using the MIH\_Net\_Group\_Manipulate request message.
3. MIHF of PoS receives the MIH\_Net\_Group\_Manipulate request message, and sends it to the MIH User using the MIH\_Net\_Group\_Manipulate.indication primitive.
4. MIH User of PoS receives the MIH\_Net\_Group\_Manipulate.indication primitive, and generates the acknowledge receipt, and sends it the local MIHF using the MIH\_Net\_Group\_Manipulate.response primitive.
5. MIHF of PoS sends the acknowledge receipt to the PoS with GM using MIH\_Net\_Group\_Manipulate response message.
6. MIHF of PoS with GM receives the MIH\_Net\_Group\_Manipulate response message, and sends it to the MIH User of PoS with GM using the MIH\_Net\_Group\_Manipulate.confirm primitive.

In Figure 6, PoS with GM sends the Certificate to each PoS



Figure 6—Transmission of Certificate

1. MIH User of PoS with GM shares the Certificate, and sends it to the local MIHF using the MIH\_Push\_Certificate.request primitive.
2. MIHF of PoS with GM sends the Certificate the MIH\_Push\_Certificate request message.
3. MIHF of PoS receives the MIH\_Push\_Certificate request message, and sends it to the MIH User using the MIH\_Push\_Certificate.indication primitive.
4. MIH User of PoS receives the MIH\_Push\_Certificate.indication primitive, and generates the acknowledge receipt, and sends it the local MIHF using the MIH\_Push\_Certificate.response primitive.
5. MIHF of PoS sends the acknowledge receipt to the PoS with GM using MIH\_Push\_Certificate response message.
6. MIHF of PoS with GM receives the MIH\_Push\_Certificate response message, and sends it to the MIH User of PoS with GM using the MIH\_Push\_Certificate.confirm primitive.

Figure 7 describes CRL sharing in Home Area Network. In this example, PoS-A having the latest CRL directly sends it with other PoS and PoS with GM under the same Home Area Network.



Figure 7—CRL sharing in Home Area Network

Figure 8 shows the command flow described in Figure 7.



Figure 8—Transmission of CRL

1. If MIH User of PoS shares the CRL, and sends it to the local MIHF using the MIH\_Revoke\_Certificate.request primitive.
2. MIHF of PoS sends the CRL to the PoS using MIH\_Revoke\_Certificate request message.
3. MIHF of PoS receives the MIH\_Revoke\_Certificate request message, and sends it to the MIH User of PoS using the MIH\_Revoke\_Certificate.indication primitive.
4. MIH User of PoS receives MIH\_Revoke\_Certificate.indication primitive, and generates the acknowledge receipt, and sends it the local MIHF using the MIH\_Revoke\_Certificate.response primitive.
5. MIHF of PoS sends the acknowledge receipt to the PoS using MIH\_Revoke\_Certificate response message.
6. MIHF of PoS receives the MIH\_Revoke\_Certificate response message, and sends it to the MIH User of PoS using the MIH\_Revoke\_Certificate.confirm primitive.
	* 1. CRL

 This sub-clause describes the CRL operation for HEMS use case.

* + - 1. CRL operation

CRL: Certificate Revocation List is a list of certificates for revoked devices. CRL is signed and distributed by the Certificate Authority.

Although the Certificate Authority is typically operated by a single service operator, in this use case, the Certificate Authority might be managed by a joint legal entity. This is because various devices developed by various manufactures need to connect each other and connect to different service, and for assuring the interoperability, it might be easier for one joint legal entity to operate the Certificate Authority which is responsible for one revocation policy.

Revocation Policy is specified by this joint legal entity. If the gross negligence occurred in the market, the joint legal entity investigates the　circumstances and decides the possibility of issuing CRL.

All devices should check the CRL regularly and confirm the validity of their own device certificates.

The CRL should be updated adequately depend on the policy of the Certificate Authority. If there should be the gross negligence in the market, the CRL would be updated more frequently than the regular policy.

 The Certificate Authority can remove the revoked certificate from the CRL depend on the life cycle of the device. For example, if maximum life time is considered to be 20 years, the Certificate Authority may remove revoked certificates from the CRL 20 years later.

* + - 1. CRL format

 The CRL is compliant with the X.509 version 2 CRL format shown in Table 2.

Table 2— CRL format

|  |  |  |
| --- | --- | --- |
| tbsCertList | 　 | 　 |
| 　 | Version | Version |
| 　 | Signature | Signature algorithm |
| 　 | Issuer | Issuer of CRL |
| 　 | thisUpdate | Update date or issue date of CRL |
| 　 | nextUpdate | Next update date of CRL |
| 　 | revokedCertificates | Revoked certificates list |
| 　 | crlExtensions | Extensions to provide methods for associating additional attributes with CRLs |
| signatureAlgorithm | 　 | Signature algorithm |
| Signature | 　 | Digital signature of CA |

* + - 1. Distribution of CRL

 All devices connected to the Internet should acquire the latest CRLs from CRL server periodically. Connection to the CRL server is established by HTTPS. Figure 9 shows the typical case where only PoS with GM can connect to the Internet. PoS with GM acquires the latest CRL from the CRL server and distributes it to the other PoS(es) .

The device has some timing flexibility to access randomly to CRL server for dispersing the peak connection to the CRL server.

 If new joining device has the latest CRLs, that device can distribute the latest CRLs to the other devices as shown in Fig.7. In this case, other PoS or PoS with GM compare their CRL and the newly distributed CRL, then, replace to the latest CRL.



Figure 9—Distribution of CRL

* + - 1. CRL handling for resource limited device

Full CRL is the CRL which contains all revoked certificates in the single list. Full CRL is easy to be handled because device should check only one single data format. However, in the large-scaled system, the data size of CRL become huge and the load for device to acquire CRL would be increased.

In the HEMS use case, it is difficult for the devices to handle large size CRL. Therefore, the size limitation of CRL is needed. The size limitation usually depends on the operation policy. Generally it should be limited in the size as device can acquire and hold. As one example, several IPTV services for consumer TV limit the size less than 10kb.

It is necessary to increase the updating frequency in order to quickly notify the revocation information to the device. However, frequent updating leads to the burden for the device which should process the large size CRL frequently. Therefore, it is required to consider the reasonable balance between the load for the device and the potential risk.

 The bellows describe various ways to reduce the size of CRL.

* Partitioned CRL

Partitioned CRL is the method to issues the large size CRL by dividing forms. Certificate Authority divides large size CRL and issues them as multiple CRLs according to the serial number of the certificate or the revocation policy.

Each divided CRL is referred to as the partitioned CRL. The CRL Distribution Points (CRLDP) field of crlExtensions specifies the location of the CRL. Device checks the CRLDP in the certificate, and determine the Partitioned CRL to be acquired. The size of each CRL can be reduced by using partitioned CRL, and notification of the location of the CRL is not needed since the location of the CRL is described in the CRLDP.

* Delta CRL

Delta CRL is used to notify the revocation information quickly. Certificate Authority issues normal CRLs (base CRLs) periodically, and issues delta CRLs at shorter intervals.

The delta CRL describes the additional revocation information from the base CRL. Device acquires the delta CRL and the base CRL. Then obtain the latest revocation information by combining those. For example, the base CRL is issued once a week, and the delta CRL is issued as the list of revoked certificates during the 24 hours once every 24hours.

* Indirect CRL

Indirect CRL is that one organization issue the CRL as one combined form by gathering the multiple CRL from the multiple Certificate Authorities. Typically CRL issuer signature is added to the indirect CRL because device should ensure the reliability of the indirect CRL issuer. The indirect CRL has an advantage that device is required to confirm only one combined CRL even if devices are using multiple CAs.

* Operational policy for exceeding the size limit

The data size of full CRL simply increases due to the addition of revoked certificates. The expired certificates are deleted from the CRL at issuing new CRL, but if the size of CRL still exceeds the limit, the latest CRL can be divided as the partitioned CRL or the old CRL near expired period can be deleted from the latest CRL according to the operation policy.

Reference

[X.509]

 ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems

 Interconnection - The Directory: Authentication Framework, June 1997.

[IETF]

　RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.