|  |
| --- |
| Input Contribution |
| Meeting ID\* | SEC17 |
| Title:\* | Relationship between Privacy Policy Manager (PPM) and oneM2M |
| Source:\* | Norihiro Okui, KDDI Corporation, no-okui@kddi.comYutaka Miyake, KDDI Corporation, yu-miyake@kddi.comNick Yamasaki, KDDI Corporation, nr-yamasaki@kddi.com |
| Uploaded Date:\* | 2015-05-12 |
| Document(s) Impacted\* | TS-0001: Functional ArchitectureTS-0003: Security Solutions |
| Intended purpose ofdocument:\* | [ ]  Decision[x]  Discussion**[x]**  Information[ ]  Other <specify> |
| Decision requested or recommendation:\* |  |
| Template Version:23 February 2015 (Dot not modify) |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

# Introduction

A concept of PPM (Privacy Policy Manager) is explained at SEC-2015-0476-Privacy\_Policy\_Manager (PPM document). The present document provides relationships between PPM and oneM2M.

The current PPM document only defines components and use case of PPM. The objective of this contribution is to provide relationship between components of PPM and components of oneM2M, and to explain which process in PPM architecture correspond to components of oneM2M.

This contribution provides explanations in the following two aspects:

* Relationship between components of PPM and components of oneM2M: This part explains relationship between four components of PPM and components of oneM2M.
* Relationship between each process of PPM and components of oneM2M: This part explains four scenarios in PPM architecture and explains relationship between steps in the scenario and components of oneM2M.

# Relationship between Components of PPM and Components of oneM2M

PPM has four components. Detail of each component is explained in PPM document (SEC-2015-0476R04-Privacy\_Policy\_Manager). This section provides relationship between these components and components of oneM2M.

1. SSO (Single Sign-On) using Pseudonymous ID
* Prevention of ID-based aggregation and protection of user privacy
* TS-0001 6.2.10 Security
* TS-0003 6.2.4 Identity Protection
1. Sophisticated consent mechanism for privacy policy
* When a user subscribes a service by an application service provider, the user becomes a data provider, and the data provider creates a privacy preference and registers it on the PPM
* This function may not be defined in oneM2M
1. Flow management of Personal Data to ASPs (Application Service Providers)
* When ASP accesses to the data in the M2M platform, the Data Flow Control function controls its access based on the privacy preference in PPM
* TS-0003 6.2.2 Authorization Architecture
* TS-0003 7.1 Access Control Mechanism
1. Traceability of personal data usage
* PPM stores the access log that records which ASPs access to what kinds of collected data
* Now, under survey.

# Relationship between each process of PPM architecture and components of oneM2M

There are four scenario in the use of PPM. This section explains relationships steps in the scenario and components of oneM2M.

* A data provider join a M2M platform
* A data provider subscribes a service by an ASP
* An ASP requests personal data that stored in a M2M platform
* A data provider checks the access log of his/her own personal data and requests for the deletion to the ASP.

## Actor

* Data Provider
	+ A user can join a M2M platform and subscribe a service by an ASP which join the M2M platform.
	+ When a user subscribe a service by an ASP, the user become a data provider.
* M2M Device
	+ A M2M device collects various kinds of data, such as sensor.
	+ A M2M device sends the data to a M2M platform.
* Application Service Provider (ASP)
	+ An ASP provides services to a user who joins the M2M platform.
	+ An ASP requests personal data from a M2M platform in order to provide services.
* M2M Platform
	+ Data Flow Control
		- ‘Data flow control’ controls various kind of data using access control policies.
	+ Portal
		- A portal is a kind of Web site or Web application in a M2M platform.
		- A user access a portal to join a M2M platform. A data provider access a portal to subscribe a service by an ASP, and to check what kind of his/her own personal data are used by ASPs.

## Flows in PPM Architecture

### Join a M2M Platform

When a data provider join a M2M platform, the data provider configures a privacy preference using the PPM. A privacy preference explains what kinds of data are allowed to access to ASPs. Figure 1 illustrates the overview of this process.

* 1. A data provider accesses a portal, and join a M2M platform.
	+ This process is equivalent to the Web access, and uses HTTP, HTTPS and so on.
	+ Outside the scope of oneM2M
	1. A data provider configure a privacy preference and register it on the PPM
	+ This process needs communications between the Portal and the PPM. These communications use HTTP, HTTPS and so on. The M2M Platform decides the protocol of these communications.
	+ Outside the scope of oneM2M



Figure 1. A data provider join the M2M Platform

### Subscribe ASP’s Service

A data provider can subscribe various kinds of services provided by ASPs in the M2M platform. Service lists are registered in the M2M platform and the data provider can select services to subscribe. When the data provider subscribes a service, the data provider needs to accept a privacy policy. In order to understand easily for the data provider, the PPM creates the customized privacy policy based on ASP’s privacy policy and the data provider’s privacy preference. Therefore, the data provider can control personal data and prevent from agreement without understanding the privacy policy. Figure 2 shows the overview of this process.



Figure 2. A data provider subscribe ASP’s service

1. A data provider access the portal and select a service to subscribe.
	* This process is equivalent to a process of access to a Web site or Web application.
	* Outside the scope of oneM2M
2. The data provider needs to accept a privacy policy to subscribe ASP’s service. The PPM creates a customized privacy policy for each data provider based on the data provider’s privacy preference.
	* It is easy for the data provider to confirm differences between the privacy preference and the customized privacy policy and to understand what kind of personal data are collected by the ASP.
	* The function of creating a customized privacy policy is outside the scope of oneM2M
3. The PPM creates access control policies based on the agreed the customized privacy policy.
	* This function may not be defined in oneM2M

### Request for the personal data to the M2M Platform

If an ASP needs personal data to provide a service, the ASP requests for the data to the M2M Platform. In this case, a data flow control retrieves access control policies from the PPM and controls the data access using them. Figure 3 illustrates the overview of this process.



Figure 3. Request for the personal data to the M2M platform

1. ASP requests for a personal data to the data flow control in the M2M platform.
	* oneM2M defines this data flow at 8.1.2 Request in TS-0001.
2. The data flow control requests for access control policies corresponding to the data to the PPM.
	* oneM2M defines this data flow at 8.1.2 Request in TS-0001.
3. The PPM responses the access control policies.
	* oneM2M defines this data flow at 8.1.3 Response in TS-0001.
4. The data flow control computes access control policies from the PPM and other, and decides whether the access is permitted or not.
	* This process can use components of 6.2.2 Authorization Architecture and 7.1 Control Mechanism in TS-0003.
5. The data flow control collects the permitted data from the database.
	* oneM2M defines this data flow at 8.1.2 Request and 8.1.3 Response in TS-0001.
6. The data flow control converts the data using pseudonymous ID. Then, the data flow control responses for the data to the ASP.
	* oneM2M defines Pseudonymous ID at 6.2.10 Security in TS-0001 and 6.3.4 Identity Protection in TS-0003.
	* oneM2M defines this data flow at 8.1.3 Response in TS-0001.
7. The data flow control creates the access log of the data and send the access log to the PPM. The PPM stores the access log
* under survey

#### Access Control Policy created by the PPM

The access control policy (ACP) is define at 6.2.2 Authorization Architecture and 7.1 Access Control in TS-0003. Figure 4 and 5 shows the overview of them.

In authorization architecture, Policy Retrieval Point (PRP) stores ACPs and responses for ACPs to Policy Decision Point (PDP) when PDP requests for ACPs to PRP.

In Figure 5, ACPs assigned to a resource. When an ASP request for a resource, PRP loads the ACPs assigned to the resource.



Figure 4. Overview of the authorization architecture (Figure 6.2.2-1 in TS-0003)



Figure 5. Relation between Resource Instances and Access Control Policies (Figure 7.1.1-1 in TS-0003)

Figure 6 shows the architecture added to the ACP created by the PPM. The PPM creates access control policies from the point of view of privacy. For example, Resource\_1 have ACP\_1 and ACP\_2 in the M2M platform without the PPM in Figure 6. Adding the PPM to the architecture, the PPM creates ACP\_3 from the point of view of privacy, Resource\_1 have ACP\_1, ACP\_2 and ACP\_3. PDP decides permission of the data using them.



Figure 6. An example of authorization architecture with the PPM

####  An example of authorization architecture with the PPM

This section explains an example of access control decision based on ACPs that are created by the PPM. Figure 7 shows the example of authorization architecture with the PPM.



Figure 7. An Example of access control decision based on ACP that is created by PPM

As a precondition, each ASP has a unique M2M-SP-ID, and ACPs are created by the PPM in advance. M2M-SP-ID is described at clause 7.2 in TS-0001. The format of ACPs are described at 7.1.3 Format of privileges and self privileges Attributes in TS-0003.

1. ASP requests for the data (dataID = 001) to the data flow control in the M2M platform.
2. Some ACPs assinged to the data. The data flow control requests for the ACPs to the PPM. (As a matter of course, the data flow control request for the other policies assigned to the data to PRP.)
3. The PPM response the ACPs to the data flow control.
4. The data flow control evaluates access request using the ACPs. (The data flow control works the role of Policy Enforcement Point and Policy Dicision Point described at 6.2.2 Authorization Architecture in TS-0003.) In this example, ACP\_u001\_d001, ACP\_u002\_d001 and ACP\_u003\_d001 assigned to the data (dataID = 001).
5. The data flow control collects the permitted data from the database. In this example, the data of (userID, dataID, data)=(001, 001, 111), (001, 001, 112), (001, 001, 113), (002, 001, 121), (002, 001, 122) are permitted data.
6. The data flow control response the data.

### Traceability of personal data usage

The PPM stores the access log of personal data. The data provider can check the status of data usage by ASPs. If the data provider would like to delete the collected data that are used by ASPs, the data provider can request the ASP to delete the data in ASP using usage records in the PPM.



Figure 8. Check the personal data usage and request deletion of the data

1. The data provider access the portal and requests for the access log of personal data. Then, the portal requests for the access log to the PPM.
* oneM2M defines this data flow at 8.1.2 Request in TS-0001.
1. The PPM responses the access log to the portal. The portal outputs the result such as a Web page using the access log.
* oneM2M defines this data flow at 8.1.3 Request in TS-0001.
* This function of the portal is outside the scope of oneM2M.
1. The data provider requests the PPM to delete the collected data.
* oneM2M defines this data flow at 8.1.3 Response in TS-0001.
1. The PPM converts the request message to make new request message for ASPs. The PPM requests ASPs to delete the collected data.
* oneM2M defines this data flow at 8.1.3 Request in TS-0001.