|  |
| --- |
| Input Contribution |
| Meeting ID\* | SEC17 |
| Title:\* | Use case of PPM (Privacy Policy Manager ):Personal data management architecture using user’s privacy preferences  |
| Source:\* | Yutaka Miyake, KDDI Corporation, yu-miyake@kddi.comNorihiro Okui, KDDI Corporation, no-okui@kddi.comNick Yamasaki, KDDI Corporation, nr-yamasaki@kddi.com |
| Uploaded Date:\* | 2015-05-10 |
| Document(s) Impacted\* | TD-0001: Use Cases CollectionsWI-0023: Study of Authorization Architecture for Supporting Heterogeneous Access Control PoliciesTR-0018: Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies 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.

# 1. Introduction

 This contribution updates the proposed use case of PPM (Privacy Policy Manager) that was submitted to the last meeting (SEC 16) as a new contribution. This contribution clarifies potential requirements to oneM2M architecture to implement the PPM.

2. Outline of PPM (Privacy Policy Manager)

(This clause is not changed from the previous contribution (SEC-2015-0476R04).)

KDDI has been researching personal data management framework based on the user’s privacy preferences and has developed the prototype system as PPM. We have adapted the PPM to large scale HEMS (Home Energy Management System) as trial, and started evaluation of PPM effectiveness.

The PPM is based on the following two main concepts:

* Based on ‘Privacy by Design’, we architect a personal data distribution base.
* Based on ‘Privacy First’, we provide users a function by which users can manage their own personal data distribution by their privacy preferences.

The PPM has the following four basic functions:

1. SSO (Single Sign-On) using Pseudonymous ID
	* The PPM provides both pseudonymous ID and SSO. Pseudonymous ID is different in each service and SP (Service Provider) identifies User with it. To avoid seeing who the user is from a pseudonymous ID, the PPM creates the ID using hash function based on cryptography.
2. Flow management of Personal Data to SPs (Service Providers)
	* Users can configure their privacy preferences, and those privacy preferences are managed at the PPM server. In other words, the users can control access right to their personal data. For example, the uses can decide which services can access their personal data, what kinds of personal data are collected, etc. Such configuration of privacy preference can be defined service by service. The users can configure their privacy preferences anytime.
	* Because configuration of privacy preference is complicated and not easy for users, we think that user support function for configuring privacy preference is required for the PPM.
3. Sophisticated consent mechanism for privacy policy
	* Before users start to use services, the users need to read and consent terms & conditions (T&Cs) and privacy policy of the services. Currently, almost services display their T&Cs and privacy policies, and users can use those services in case the users agree them. Because the PPM assumes that the user can select the kinds of providing personal data to the service, interactive agreement process is implemented. Moreover, reading T&Cs and privacy policy is troublesome, and many users do not read them completely. So emphasis mechanism of important part for each user is important. Such customization of T&Cs and privacy policy for each user can be done based on user’s privacy preference.
	* In this procedure, the PPM update user’s privacy preference based on his/her answers.
4. Traceability of personal data usage
	* The PPM has logging function of personal data flow. By visualizing personal data usage from logged record, the user can recognize the situation of correct use of his/her personal data. Moreover the users can request service providers to delete their personal data based on data access record.

3. Use case of the PPM (draft)

Title: Personal data management mechanism based on user’s privacy preference

XX.X.1. Description

Because the data collected by the M2M platform may include personal information or sensitive information of data providers, the access to such data should be controlled appropriately. This use case shows the data management mechanism based on data provider’s privacy preferences, which is developed as a PPM (Privacy Policy Manager). Because access from service providers to the collected data at M2M service platform is controlled based on the privacy preferences that are configured by data providers, unnecessary and unwanted access to the collected data is blocked appropriately. This use case is describes based on HEMS service.

XX.X.2. Source

KDDI Corporation

XX.X.3. Actors

* Front-end data-collection equipment (M2M devices)
	+ This actor collects various kinds of data and sends the data to a management platform. The collected data may include sensitive or privacy information of data providers.
* Management platform (M2M Service Provider’s Platform)
	+ The management platform stores the data collected by M2M devices. This also manages the access control to the stored data.
* Data provider
	+ A data provider is a user of services from application service providers. The user subscribes services, and the management platform starts to collect data related to the user and its services. In case that a service requires personal information of a user, such data are collected by the management platform. So the user becomes the data provider.
	+ The data that are provided by the data provider may include sensitive or private information. The data provider can configure his/her privacy preference for the collected personal data. If the data provider would not like to permit the application service provider to access specific kinds of collected data, the data provider can configure the privacy preference of the service to control the access. The management platform control the access from the application service providers to the collected personal data based on the privacy preferences.
* PPM
	+ A PPM function manages privacy preferences of the data providers. The data providers configure their privacy preferences for subscribing application services. The application service providers present the data providers which kinds of data are used by the application service, and the data providers configure their privacy preferences to give access permissions to several kinds of collected data. Although an application service may use many kinds of data from a data provider, the data provider can permit the subset of listed data by configuring the privacy preference for its application service.
	+ A PPM function also has mechanism to record the usage of the collected data. When application service providers access to the collected data from data providers, its accesses are logged to the PPM. If the data providers would like to refer the past usage of their personal data, they can check it by accessing the PPM. The data provider can request the application service providers to delete the collected data based on the record of access log.
* Application service providers
	+ This actor provides many kinds of services to service users. In case the application service providers use the data stored in the management platform, they access to the data via data flow control function. Because this function provides access control to the data, the function asks a Policy Decision Point and decides whether the application service provider has access permission to the accessing data or not. The Policy Decision Point computes the access rights based on several policies including the privacy preferences in the PPM.

XX.X.4. Pre-conditions

 None

XX.X.5. Triggers

* Service subscribing trigger: configuring privacy preference of data providers for each service
* Data collection trigger: collecting data at M2M modules
* Data access trigger: accessing collected data from application service providers
* Data usage reference trigger: referring usage of collected data from application service providers
* Data deletion trigger: requesting deletion of accessed and stored data in application service providers

XX.X.6. Normal Flow

The following normal flow is described based on a figure in High Level Illustration (XX.X.9).

(a) Configuration of privacy preference by data provider

1. When a user starts to subscribe a service of application service provider, the user checks the privacy policy of service. The privacy policy explains what kinds of data will be accessed to provide the service. If the user permits the application service provider to access the collected data by M2M management platform, the user becomes the data provider.
2. The data provider can select the kinds of data that the application service provider can access. If the data provider would not like to permit the application service provider to access specific kinds of data, the data provider can configure the privacy preference to enable this situation. In other words, because this access permission can be defined item by item, the data provider can restricts the access to the part of collected data.

 (2) M2M data collection

1. The M2M Service Provider’s platform collects data related to the data providers by using M2M devices.

 (3) M2M data access from application service providers

1. When application service providers access to the collected data in M2M Data, they access to the Data Flow Control at first. The Data Flow Control has a function of policy enforcement, and it accesses to the Policy Decision Point to judge the access permission based on access policies. The Policy Decision Point retrieves access policies and privacy preference to the target data from policy data base and PPM respectively. It computes access permission to the target data from the retrieved policies and privacy preference, and returns the results to the Data Flow Control.
2. If the access is permitted, the Data Flow Control transfers the target data to the application service provider. If the access is not permitted, the Data Flow Control responds to the application service provider with the notification of access denied with reasons.

 (4) Traceability of personal data usage

1. When the application service providers access to the collected data in M2M Data, all the access and its result (access permitted, access denied) are recorded and stored at the PPM.
2. If the data provider would like to check the status of data usage by application providers, the data provider access to the PPM. The data provider can recognize that which application provider accessed to what kinds of collected data.
3. If the data provider would like to delete the collected data that were stored in the application service providers, the data provider can request the application service providers to delete the transferred data by specifying access record in the PPM.

XX.X.7. Alternative Flow

 None

XX.X.8. Post-conditions

 None

XX.X.9. High Level Illustration



Figure x-xx Overview of Personal Data Management mechanism using PPM

1. When a user starts to subscribe a service from an application service provider, the user checks the privacy policy and recognizes what kinds of data are used in this service. If the user permits the application service provider to use the collected data related to the user, the user becomes the data provider. The user can select the data items that the application service provider can access. This is controlled by configuring privacy preference for its service.
2. When the data provider configures the privacy preference for the service, PPM function receives the list of data that the service uses. The data provider selects the data items from this list for controlling the access to the collected data.
3. M2M devices collect various kinds of data from the data providers.
4. The collected data are transferred to the M2M Service Provider’ Platform.
5. The collected data from the M2M Network are stored in M2M Data.
6. The Application Service Providers access to the collected data in M2M Data via Data Flow Control. The Data Flow Control controls access to the data based on the privacy preference and other polices.
7. The Data Flow Control retrieves access control information from Policy Decision Point.
8. The Policy Decision Point computes the access control list for the target data by using the privacy preference in the PPM and other policies, and returns the results to the Data Flow Control.
9. The Data Flow Control records all accesses from the application service providers to the collected data in M2M Data and its record is logged at the PPM.

XX.X.10. Potential Requirements

* The M2M system shall support the capability of managing the collected data by using access control mechanism to avoid unnecessary and unwanted personal information access.
	+ The access control mechanism shall have capability to handle privacy preferences that was configured by data providers.
	+ The M2M Service Provider’s Platform shall have a function to record the data flow by application service providers to enable the data providers to trace the status of data usage.
	+ The M2M Service Provider’s Platform shall have a function to request the application service providers to delete the specified collected data that are stored in the application service providers.