|  |
| --- |
| Input Contribution |
| Meeting ID\* | SEC16 |
| Title:\* | PPM (Privacy Policy Manager ): Personal data management architecuture using user’s privacy preferences  |
| Source:\* | Yutaka Miyake, KDDI Corporation, yu-miyake@kddi.comRyu Watanabe, KDDI Corporation, ry-watanabe@kddi.comNick Yamasaki, KDDI Corporation, nr-yamasaki@kddi.com |
| Uploaded Date:\* | 2015-03-20 |
| 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: Functinal 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

 A concept of PPM (Privacy Policy Manager) and its relationship with oneM2M were introduced at the SEC15.1 and SEC 15.2 meetings. This contribution provides draft text of use case using the PPM and summarizes relationship between oneM2M documents and the PPM.

2. Outline of PPM (Privacy Policy Manager)

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 (first draft)

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

XX.X.1. Description

Because the data collected by the M2M system may include personal information or sensitive information of users, the access to such data should be restricted and controlled appropriately. This use case shows the data management mechanism based on user’s privacy preferences, which is developed as PPM (Privacy Policy Manager).

XX.X.2. Source

KDDI Corporation

XX.X.3. Actors

* Front-end data-collection equipment (M2M devices)
* Management platform (M2M Service Provider’s Platform)
* PPM server
* Application Service providers

XX.X.4. Pre-conditions

 None

XX.X.5. Triggers

* Data collection trigger: collecting data at M2M modules
* Data access trigger: accessing collected data from service providers

XX.X.6. Normal Flow

1. The users configure their privacy preferences at the PPM server based on the terms and conditions (T&C) and privacy policy of application service providers.
2. Data are collected and stored to the M2M service provider’s platform according to the privacy preferences in the PPM server.
3. When an application service provider accesses to the stored data that were collected by M2M module, its access is controlled based on the user’s privacy preference in the PPM server.

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

* Users configure their privacy preference to the PPM (Privacy Policy Manager).
* Collected data used by M2M modules are sent to the M2M Service Provider’s Platform via M2M network.
* Data Flow Control part of M2M Service Provider’s Platform stores the data to storage according to user’s privacy preference in the PPM.
* When application service providers retrieve the data from M2M data storage, they access to the PPM and get the access right to the M2M data. If the access is permitted based on the user’s privacy preference, the PPM issues access tokens to the service providers.
* The application service providers access to M2M Data through Data Flow Control part with the access token. The Data Flow Control part manages data flow based on token’s permission.
* Theses flows are logged at the Data Flow Control function. If a user would like to check the usage of his/her personal data, the user can check the status from the stored log data.

XX.X.10. Potential Requirements

* The M2M system shall support the capability of managing the personal data flow based on the user’s privacy preferences.
	+ The data collection by M2M modules shall be controlled based on the user’s privacy preferences.
	+ The access to the collected data from application service providers shall be controlled based on the user’s privacy preferences.
	+ The flow of personal data shall be recorded, by which users can check the usage of their personal data at the application service providers.

4. Relationship between PPM and oneM2M activities

The following documents are related to the PPM.

* TS-0001: Functional Architecture
* TS-0003: Security Solutions
* WI-0023/TR-0018: Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies

4.1 Functional Architecture for Security (6.2.10 in TS-0001)

Security (SEC) CSF comprises the following functionalities:

* Sensitive data handling;
* Security administration;
* Security association establishment;
* Access control including identification, authentication and authorization;
* Identity management.

These functionalies can be used for realizing the PPM concept. Following sections identify the relationship between PPM requirements and those functionalities.

4.2 Identity Protection (6.2.4 in TS-0003)

Identity protection is provided in 6.2.4 [TS-0003]. This clause says “Identity Protection provides services to the Application Layer such as pseudonyms and protecting the anonymity of transactions.” This function can satisfy the requirement of PPM for pseudonymous ID.

4.3 Authorization (7 in TS-0003) and Authorization Architecture (6.2.2 in TS-0003)

Access control mechanism based on policy is described in 7 and 6.2.2 [TS-0003]. This mechanism can be used to control personal data flow based on user’s privacy preference. Because the PPM assumes token based access control, access control mechanism based on this authorization architecture may be required.

4.4 Access control policy (WI-0023/TR-0018)

TR-0018 provides candidate security solutions for authorization architecture, authorization procedures and access control policies. Although almost contents in current version of TR-0018 are empty, some of clauses are related to the PPM, such as authorization architecture, specification of access control policies and access control policy languages.

4.5 Information Recording (12 in TS-0001)

Information Recording is described in clause 12 [TS-0001]. In order to satisfy a traceability requirement of PPM, the part of this function can be used.

4.6 Required additional functions for PPM

In order to realize personal data management framework based on the PPM concept, the following functions are needed to be defined.

* Management of privacy preference mechanism
* Data flow management (including appropriate access control mechanism) based on privacy preference
* Logging function of data flow (access record)
* Unified format for Terms & Conditions and Privacy Policy, and its customization mechanism