|  |
| --- |
|  |

|  |  |
| --- | --- |
| Input Contribution | |
| Meeting ID\* | SDS#47 |
| Title:\* | GDPR feature analysis and impact to oneM2M |
| Source:\* | JaeSeung Song, KETI, jssong@sejong.ac.kr  Minbyeong Lee, Hyundai Motors, [minbyeong.lee@hyundai.com](mailto:minbyeong.lee@hyundai.com) |
| Date:\* | 2020-09-28 |
| Input related to\* | WI-0095 oneM2M System Enhancement to Support Privacy Data Protection Regulations (eDPR)  TR-0062 V 0.2.0 |
| Intended purpose of  document:\* | Decision  Discussion  Information  Other <specify> |
| Impacted other TS/TR(s) |  |
| Decision requested or recommendation:\* | Agree for inclusion in TR-0062 |
| Template Version: January 2017 (Do 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

This contribution provides input about key issue on consent management for GDPR.

### -----------------------Start of change 1-------------------------------------------

# 8 Proposed Solutions

*Editor’s Note: The section provides solutions to the required functions identified in the previous section.*

## 8.x Solution: Key Issue x – Consent Management

Under GDPR, processing personal data is generally prohibited, unless it is expressly allowed by law, or the data subject has consented to the processing by the owner of the data. According to GDPR, consent must be freely given, specific, informed and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. Therefore, it is very important how to manage consent in IoT platforms.

oneM2M system supports access control policy (ACP) to handle the access right of the resources containing data. However, the current ACP is limited to support the concept consent management introduced by GDPR as it only defines the access right of the originator for the given operations (i.e., CRUDN).

In GDPR, Consent is defined in Article 4(11) as: “any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. On the other hand, ACPs in oneM2M are used by the CSE to control access to the resources. This means that ‘Consent’ and ‘ACPs’ can complement each other as ACPs control the access of the resources, while consent further defines what kinds of processing are allowed on personal data within the resources.

In order to support the concept of consent management from GDPR, oneM2M system should answer the following two questions:

* How to provide consent from the users?
* How to manage consent information?

Consent is strictly related to data processing as it gives a clear indication about which is the purpose that the personal data of a user is processed for. Each processing purpose is associated with one or more processing activities. Basically, individuals who hold IoT data want to limit their consent. Assume that as an IoT service platform provider, a data holder wants to use collected IoT data for various purposes, including marketing purposes. Here are some examples of various consents.

* Customer A agrees to share personal bio data measured by wearable IoT devices to specific hospitals.
* Customer B agrees to use personal location data to be used by marketing companies after three months from now.
* Customer C agrees to forward personal data from IoT devices to 3rd party data analytics companies and receive recommendations.

**Provisioning of consent:**

As IoT platforms need to get users’ consent for their data, there should be clear and easy ways to acquire consent from users. There exist three different ways to get it from IoT service platforms.

1. Pre-provisioning: When a user purchases an IoT device from a service provider, consent can be given and embedded to the IoT device. When the device is registered to an IoT platform, the pre-provisioned consent can be included in the registration procedures.
2. Post-provisioning: An IoT application is registered to an IoT platform without consent. Once the data of the IoT application is identified as personal data, a user can select its consent via, for example, a web interface IoT application.
3. Interactive-provisioning: When an IoT application is registered to an IoT platform, there should be an additional step acquiring users’ consent.

Below table shows the differences between three consent provisioning mechanisms.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Post-provisioning** | **Pre-provisioning** | **Interactive-provisioning** |
| Who | User | User or Service Provider | User |
| When | After registration | At purchasing IoT device | During registration |
| How | Using UI (e.g., Web UI) | Using pre-configured message | Using enhanced registration procedures |

### 8.x.1 Consent Management Solution #1

**Consent management dedicated resource:**

Consent should include various information to make the purpose and associated activities clearly. Such activities and information can be modeled as a resource called [*consentMgt*]. Each resource identified as personal data refers to associated consent resources. The following figure introduces a high-level concept of consent management.



Figure 8.x.1-1. Consent management concept

The [*consentMgt*] resource is used to store consent purposes and relevant information.



Figure 8.x.1-2: Structure of [*consentMgt*] resource

The *[consentMgt]* resource shall contain the attributes specified in the table below.

Table 8.x.1-1: Attributes of [consentMgt] resource

| Attributes of *[consentMgt]* | Multiplicity | RW/  RO/  WO | Description |
| --- | --- | --- | --- |
| *holderID* | 1 | RO | The holder of the consent. |
| *holderGroupIDs* | 0..1 (L) | RW | A list of groups that the holder of this consent belongs, for example,   * Business * Consumer * Administrator * VIPs |
| *creationTime* | 1 | RO | Indicate when this consent is created. |
| *consentName* | 1 | WO | The name of this consent. |
| *allowedProcessing* | 0..1 (L) | RW | A list containing allowed processing, for example,   * Sharing with 3rd party * Marketing |
| *validity* | 1 | RW | Indicate the validity of this consent. |
| *consentID* | 1 | WO | The identifier of this consent. |
| *consentGroups* | 0..1 (L) | RW | A list of consent groups that this consent belongs, for example,   * Specific applications * Marketing campaigns * Cookie type of consents |
| *expirationTime* | 1 | RO | The expiration time of this consent. |
| *rightToWithdraw* | 1 | RW | Indicate whether the holder has a right to withdraw the consent at anytime. |

### 8.x.2 Consent Management Solution #2

**ACP-based consent management:**

Consent can be considered as part of the access control policy as it handles a data holder’s intention about data usage. If contents of data are related to personally identifiable information, only contents with users’ consent can be shared or used by others except for the holder of data. Therefore, the consent can be considered as one of ACP. Therefore, in this section, a solution enhancing the existing ACP mechanism to cover the consent management is introduced.

The existing <accessControlPolicy> resource is comprised of *privileges* and *selfPrivileges* attributes which represent a set of access control rules defining which entities (defined as *accessControlOriginators*) have the privilege to perform certain operations (defined as *accessContolOperations*) within specified contexts (defined as *accessControlContexts*) and are used by the CSEs in making Access Decision to all or specific parts (i.e. child resources or attributes) of the targeted resource (defined as *accessControlObjectDetails* and *accessControlAttributes*).

In the case of consent management, it is important to define what kinds of processings are allowed by the service provider. Therefore, an additional attribute called *consentRules* can be introduced to define a set of consent management rules that applies to resources referencing this <accessControlPolicy> resource.

For example, the following table that is copied from TS-0001 shows the attributes of <accessControlPolicy> resource.

Table 8.x.2-1: Attributes of *<accessControlPolicy>* resource from TS-0001

| Attributes of *<accessControlPolicy>* | Multiplicity | RW/  RO/  WO | Description | *<accessControlPolicyAnnc>* Attributes |
| --- | --- | --- | --- | --- |
| *resourceType* | 1 | RO | See clause 9.6.1.3. | NA |
| *resourceID* | 1 | RO | See clause 9.6.1.3. | NA |
| *resourceName* | 1 | WO | See clause 9.6.1.3. | NA |
| *parentID* | 1 | RO | See clause 9.6.1.3. | NA |
| *expirationTime* | 1 | RW | See clause 9.6.1.3. | MA |
| *labels* | 0..1(L) | RW | See clause 9.6.1.3. | MA |
| *creationTime* | 1 | RO | See clause 9.6.1.3. | NA |
| *lastModifiedTime* | 1 | RO | See clause 9.6.1.3. | NA |
| *announceTo* | 0..1 (L) | RW | See clause 9.6.1.3. | NA |
| *announcedAttribute* | 0..1 (L) | RW | See clause 9.6.1.3. | NA |
| *announceSyncType* | 0..1 | RW | See clause 9.6.1.3. | MA |
| *owner* | 0..1 | RW | See clause 9.6.1.3 | NA |
| *privileges* | 1 | RW | A set of access control rules that applies to resources referencing this *<accessControlPolicy>* resource using the *accessControlPolicyID* attribute. | MA |
| *selfPrivileges* | 1 | RW | A set of access control rules that apply to the *<accessControlPolicy>* resource itself and *accessControlPolicyIDs* attribute of any other resource which is linked to this <accessControlPolicy> resource. | MA |
| *consentRules* | 1 | RW | A set of consent management rules that applies to resources referencing this <accessControlPolicy> resource | NA |
| *authorizationDecisionResourceIDs* | 0..1 (L) | RW | A list of addresses of <*authorizationDecision*> resources. See clause 9.6.41 for further details. | MA |
| *authorizationPolicyResourceIDs* | 0..1 (L) | RW | A list of addresses of <*authorizationPolicy*> resources. See clause 9.6.42 for further details. | MA |
| *authorizationInformationResourceIDs* | 0..1 (L) | RW | A list of addresses of <*authorizationInformation*> resources. See clause 9.6.43 for further details. | MA |

The set of consent management rules represented in *consentRules* attributes are comprised of consent-management-rule-tuples (*consentHolder*, *createdTime*, *consentName, allowedProcessing, consentValidity, expirationTime, rightToWithdraw*) with parameters shown in Table 8.x.1-1 which are described in the previous clauses 8.x.1.

The following Figure 8.x.2-2 shows a high-level concept of consent management using the <accessControlPolicy> resource.



Figure 8.x.2-2. ACP-based consent management concept

### -----------------------End of change 1-------------------------------------------