|  |
| --- |
| Input Contribution |
| Meeting ID\* | RDM #40 |
| Title:\* | Use case on Volatile data management service |
| Source:\* | Youngjin Na, Hyudai Motor, jkim@hyundai.com Min-Byeong Lee, Hyundai Motor, minbyeong.lee@hyundai.com JaeSeung Song, KETI, jssong@sejong.ac.kr  |
| Date:\* | 2019-05-13 |
| Input related to\* | TR-0026 (Rel-4) |
| Intended purpose ofdocument:\* | [x]  Decision[ ]  Discussion[ ]  Information[ ]  Other <specify> |
| Impacted other TS/TR(s) |  |
| Decision requested or recommendation:\* | Agree for inclusion in TR-0026. |
| 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 new use case on Volatile data management service to Clause 6 “Vehicular Domain Use Cases” in TR-0026.

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

## 6.x Volatile Data Management for Instant IoT Services

### 6.x.1 Description

Currently, oneM2M system supports expiration timer to delete the resource from the Hosting CSE after a certain amount of time/date. This attribute can be used by IoT services utilizing temporary access. Using the expiration timer, a resource can be deleted after a given time duration. However, the current oneM2M mechanism deleting a specific resource is very limited to support various emerging IoT/M2M applications.

Now a days many IoT or new services supporting self-deleting feature because of security and privacy reason. Several examples are listed below:

* *“Snapchat” similar IoT applications*: if received data is read by user, the data is deleted within 10 sec. if not read by the user, data is deleted after 24 hours.
* *Security & Privacy related IoT services*: any data associated with personal information shouldn’t be shared by others. Data shouldn’t be stored in a platform.
* *Medical and wearable IoT services*: only a dedicated doctor can read medical data from the platform. Then the data should be removed.

As many IoT services need a feature handling some data with an instant manner, volatile data management function can be considered as a common function.

### 6.x.2 Source

RDM-2019-0046-Use\_case\_for\_Volatile\_Data\_Management\_Service

### 6.x.3 Actors

* Vehicle: An application sending various data generated from a vehicle and driver.
* Cloud Node: A node that handles and manages data from vehicles.
* Instant Application: An application that consumes data from the Cloud Node.

### 6.x.4 Pre-conditions

* A vehicle is equipped with sensor and device to collect data from the driver and the vehicle.
* Data stored in the Cloud IoT platform should be consumed by a designated application.
* Data annotated with a volatile feature should be stored in a platform after a certain critaria is satisfied. For example, data should be removed from the platform after it is read by the designated application.

### 6.x.5 Triggers

* A vehicle measures various data from its internal sensors and sends the measured information to the IoT cloud platform with additional information classifying volatile data and criteria for self-deletion.

### 6.x.6 Normal Flow

Figure 6.x.6.1 illusrates the high-level flows of EDR service with volatile feature use case, which consists of the following steps:

* **Step 001**: IoT sensors equipped with a moving vehicle send measured data to the IoT platform with a volatile feature that is comprised of indication of volatile data type, criteria describing the condition for performing self-deletion and access right.
* **Step 002:** IoT service layer platform creates the request resource to store measured data. Data configured with the volatile feature should be distingushied from other normal resourses so that these resource can be deleted once the given condition is satisfied. For example, the criterial can be given such as “Delete the resource when just after the resource is read by Application #2”.
* **Step 003:** IoT service layer platform returns response message to Application #1
* **Step 004:** Application #2 retrieves the data from the resource previously configured with the volatile feature.
* **Step 005:** IoT service layer platform returns response message containing measured data to Application #2. IoT service layer platform increases a read counter for the resource. This read counter is an additional attribute for the resource to provide information how many times read by consumers.
* **Step 006:** As the resource is configured with the volatile feature and the condition is satisfied (i.e., the resource is read by Application #2 that has a proper access right to the resource), the IoT service layer platoform delete the resource.



**Figure 6.x.x.6.1: Normal flow for volatile Event Data Recorder (EDR) data management service**

### 6.x.7 Alternative Flow

None

### 6.x.8 Post-conditions

None

### 6.x.9 High Level Illustration



Figure 6.x.9.1: High level illustration of EDR data management with volatile feature

### 6.x.10 Potential requirements

1. oneM2M System shall be able to track the number and types of operations on oneM2M resources
2. oneM2M System shall be able to delete a resource based on resource deleting policy (e.g., delete a resource when the resource is read by a specific application)

### -----------------------End of Change 1 ---------------------------------------------

Copy and paste the potential requirements to Section 7

# 7 Overview of Potential Requirements

Potential requirements from all vehicular domain use cases collected in this technical report are summarized as follows,

1. The M2M application System shall enable the M2M Devices to exchange M2M application to diagnostic data periodically with the M2M Application in the network domain ([i.2] OSR-118).

NOTE 1: This requirement addresses the use case 6.1.

1. The M2M System shall enable the M2M Application to configure the notification interval in the M2M Devices ([i.2] OSR-112).

NOTE 2: This requirement addresses the use case 6.1.

x) oneM2M System shall be able to track the number and types of operations on oneM2M resources.

NOTE x: This requirement addresses the use case 6.x.

x) oneM2M System shall be able to delete a resource based on resource deleting policy (e.g., delete a resource when the resource is read by a specific application)

NOTE x: This requirement addresses the use case 6.x.