|  |
| --- |
|  |

|  |
| --- |
| Input Contribution |
| Meeting ID\* | RDM#52 |
| Title:\* | Use case on disguising data for security and privacy |
| Source:\* | JaeSeung Song, KETI, jssong@sejong.ac.krMinbyeong Lee, Hyundai Motors, minbyeong.lee@hyundai.com Franck Le Gall, EGM, Franck.le-gall@egm.io  |
| Date:\* | 2021-12-06 |
| Input related to\* | TR-0001 (Rel-5) |
| Intended purpose ofdocument:\* | [x]  Decision[ ]  Discussion[ ]  Information[ ]  Other <specify> |
| Impacted other TS/TR(s) |  |
| Decision requested or recommendation:\* | Agree for inclusion in TR-0001.  |
| 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 introduces a new use case for disguising data for privacy and security.

R01: Added sentences to clarify the following points:

* Add background information about this use case (e.g., GDPR k-anonymity)
* Add a reference about GDPR and k-anonymity

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

## 7.2 Use case #x – Disguise Data for Security and Privacy

### 7.2.1 Description

A smart home can monitor and control everything in various fields such as home appliances (e.g., TV, air conditioner, refrigerator), energy consumption devices (e.g., water, electricity, air conditioning), and security devices (e.g., door lock, surveillance camera) through a communication network.

While it may be convenient to control a smart home from a remote device (such as a smartphone), there are many cases of how critical security devices like locks, alarms, and even baby monitors can be hacked. If the smart home is hacked or the smart home data set is shared with the public, smart home devices like smart plugs or lightbulbs can provide entry points for hackers. For example, hackers can easily predict when the house is vacant by analyzing the data measured by smart home devices.

The k-anonymity algorithm is a basic model for personal information protection and can be used as one of the methods to ensure anonymity, which is one of the personal information protection methods suggested by GDPR. In other words, guaranteeing anonymity means a technology that makes it impossible to identify a specific individual in a dataset containing personal information. A technology that prevents specific personal information from being exposed by creating it is also used. K-anonymity is a technology that makes it impossible to extract personal information or specific information by easily combining different information and ensuring that at least k of the same value exists in a given data set. To this end, in k-anonymity, a part of the data set is modified, or arbitrary data is added so that all data have the same (or indistinguishable) k-1 or more data as themselves. Therefore, it is impossible for an attacker to know which data is being attacked in an unidentified data set.

### 7.2.2 Source

### [General Data Protection Regulation (GDPR)](https://gdpr-info.eu/) [i]

### 7.2.3 Actors

* Smart home sensors: Sensors deployed in smart home.
* IoT platform: An IoT platform that manages data from smart home applications

### 7.2.4 Pre-conditions

* The cloud IoT platform awares which IoT applications are subject to be protected.

### 7.2.5 Triggers

For example, a smart home measures various data from its deployed sensors, e.g., termperature, humidity, status of door. As data from these smart home sensors can reveal user’s behavior, the IoT service cloud platform generates a set of fake data that is visible to others except for the home family member.

### 7.2.6 Normal Flow

Figure 7.2.6-1 illusrates the high-level flows of the generating fake data for security and privacy use case, which consists of the following steps:

* **Step 001**: IoT sensor (i.e., Application #1) in a smart home measuring temperature sends measured data to the IoT platform. The resource for Application #1 is configured to generate a fake data when a new measurement is created.
* **Step 002:** IoT service layer platform creates a resource to store the new measurement. Then IoT service layer platform returns response message to Application #1
* **Step 003:** Application #1 sends a request to create a resource which is a placeholder for new data measurement.
* **Step 004:** As the application resource is configured to generate a fake data when there is a new measurement, a data management function is informed internally.
* **Step 005:** The data management function creates a resorce for a fake data and store a fake value to the resource.
* **Step 006:** IoT service layer returns a response message to Application #1.



Figure 7.2.6-1 A normal flow for creating fake data when a new measurement is created

### 7.2.7 Alternative Flow

None

### 7.2.8 Post-conditions

None

### 7.2.9 High Level Illustration



Figure 7.2.9-1 Conceptual diagram of hiding trends of data over time using fake data

### 7.2.10 Potential Requirements

1. The oneM2M System shall be able to generate fake data for security and privacy reason (e.g., hide trends of smart home data change).

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