|  |  |
| --- | --- |
| Input Contribution | |
| Meeting ID\* | SDS 41 |
| Title:\* | Privacy control |
| Source:\* | Dale Seed, Convida, [Seed.Dale@convidawireless.com](mailto:Seed.Dale@convidawireless.com) |
| Date:\* | 2018-06-30 |
| Input related to\* | WI-0077 |
| Intended purpose of  document:\* | Decision  Discussion  Information  Other <specify> |
| Impacted other TS/TR(s) | TR-0050-v0.8.0 |
| Decision requested or recommendation:\* | Approval of the privacy control solution |
| 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 proposes a privacy control solution which extends and build upon the attribute-level access control policy enhancement that was already accepted into TR-0050.

Note – At TP39 contribution SDS-2019-0066 was agreed but was not properly integrated into the baseline of TR-0050. The Rapporteur of TR-0050 has been notified of this. This contribution further builds upon this agreed contribution.

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

### 7.3.X Solution #2.1: Attribute-Level Privacy Policy Solution

#### 7.3.X.1 Introduction

This solution addresses key issue #2.1: Support for privacy policies.

This solution further enhances the attribute-level access control rules solution proposed in clause X.Y.Z to support additional privacy functionality.

#### 7.3.X.2 Solution details

The attribute-level access control solution proposed in clause X.Y.Z of this specification already supports the privacy capability to filter specified attributes from a resource representation that is shared with a request Originator based on the definition of a new accessControlAttributes parameter within the oneM2M access control policy.

This solution proposed to further enhance the accessControlAttributes parameter to add additional privacy capability. As shown in Table 7.3.X.2-1, in addition to the name of an attribute, each element in the list of accessControlAttributes can also include an optional indicator whether the value of the named attribute requires anonymization by the Hosting CSE or not. If required, then the Hosting CSE can anonymize the value before returning it in a response to the request Originator. This anonymization functionality can help ensure the privacy of the information contained within the attribute is maintained while at the same time still allowing useful data to be shared with the Originator. This provides an alternative to filtering of attributes.

Note, the method and type of anonymization performed by the Hosting CSE is outside the scope of this specification.

Table 7.3.X.2-1: Parameters of an accessControlAttributes element

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Usage Description | Mandatory/Optional | Format |
| attribute | The name of the attribute applicable to this rule | M | Name of resource attribute |
| anonymizationRequired | An indicator whether the value of the named attribute requires anonymization by the Hosting CSE when it is returned to a request Originator. | O | TRUE or FALSE  Default is FALSE |

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