|  |
| --- |
| Input Contribution |
| Meeting ID\* | SEC 31 |
| Title:\* | Use Case 3 - Enrollment using App-ID metadata |
| Source:\* | Ian Deakin, iconectiv, ideakin@iconectiv.com  |
| Date:\* | 2017-09-21 |
| Input related to\* | WI-0073 - App-ID Registry Function |
| Intended purpose ofdocument:\* | [x]  Decision[ ]  Discussion[ ]  Information[ ]  Other <specify> |
| Impacted other TS/TR(s) | NA |
| Decision requested or recommendation:\* | Approve this section to the TR  |
| 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.

# 5.x Use Case : Registration Enrollment using the App-ID Metadata

### 5.x.1 Description

Where the connecting IoT application (AE-ID/App-ID ) is unknown to the oneM2M system, the administrator of the system, must configure the IoT application identity service subscription rule <serviceSubscribedAppRule> to allow the IoT application to connect with the Service Provider infrastructure and provide its data.

The <serviceSubscribedAppRule> resource represents a rule that defines allowed Role-ID, App-ID and AE-ID combinations that are acceptable for registering an AE on a service providers infrastructure.



**Figure 5.x.1-1: Service Subscription App Rule**

The rule contained in a <serviceSubscribedAppRule> resource defines a mapping between:

a) one or more Credential-ID(s); and

b) combinations of one or more Role-ID(s), one or more App-ID(s) and one or more AE-ID(s) which are allowed to be used for registering AE(s) that issued a registration request via a Security Association established with the credentials associated with the Credential-ID(s)

Today if the Service Provider has no prior knowledge of the IoT application (AE-ID/App-ID ) then the IoT application will not authenticate and the administrator would need to manually configure the <serviceSubscribedAppRule>. This presents issues for both scale through mass enrolment and/or enrolment of unknown IoT applications.

**Using App-ID Registry Function to auto enroll <serviceSubscribedAppRule**>

By connecting with the App-ID Registry Function, the service provider infrastructure can query the metadata for a presented IoT application’s (AE-ID/App-ID ) to auto-populate the service subscription.

Where the AE-ID/App-ID are unknown to the SP infrastructure. Using the App-ID Registry Funtion will enable the <serviceSubscribedAppRule> to be auto-populated from the metadata provided from the App-ID Registry Function.