|  |  |
| --- | --- |
| Input Contribution | |
| Meeting ID\* | SEC 31 |
| Title:\* | Use Case 2 - Allow Certified IoT applications |
| Source:\* | Ian Deakin, iconectiv, ideakin@iconectiv.com |
| Date:\* | 2017-09-21 |
| Input related to\* | WI-0073 - App-ID Registry Function |
| Intended purpose of  document:\* | 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 : Allow Certified IoT applications

### 5.x.1 Description

Some specific IoT services rely strictly on industry certification for the use of any IoT application. The IoT application not only needs to be fit for purpose, but must comply with specific industry regulation, technical specification, consumer rights and industry specific security policies. For example a power station may require strict environmental and security compliance for its use

To this end, test and certification bodies provide services to ensure that an IoT application are conformant with the appropriate specifications for compliance.

Today a Service Provider has no context of an unknown IoT application being compliant with any specific certifications or not. I.e. is a heart rate monitor or blood pressure monitor certified and should the data be allowed to be passed into the client’s health record. The consequence of such could be damaging not only to the patient, the credibility of the health care provider and IoT service provider

**Using App-ID Registry Function to verify the IoT application is certified for use.**

The service provider infrastructure can verify the identity of a connecting IoT application is certified for use and fit for purpose, with the App-ID Registry Function. The SP is able to query the App-ID Registry Function if the App-ID is registered and if so collect the metadata for a presented IoT application’s (AE-ID/App-ID). The App-ID metadata can contain information to enable the SP to verify if the connecting IoT application is certified for the specific use. The App-ID metadata can contain the following attributes to allow the SP be informed regarding the certification status and to make decisions how to allow the IoT application connect, if at all :-

* **Certification body**: the test and certification body that has verified the App-ID capability and the metadata profile.
* **Certification compliance**: List of the compliance functionality that is certified by the certification body. Not all features of the certification process may be compatible with the IoT application. It is possible only a sub set of features are compliant with the certification process.

Using the App-ID metadata provided by the App-ID Registry Function, the SP infrastructure can verify the App-ID certification compliance of the connecting IoT application and if it should be allowed to connect and provide data for the IoT service.

The role of the App-ID Registry Function is not to enforce the policy of the SP infrastructure, but for the SP infrastructure to be informed through the App-ID metadata profile to automate the authentication and enrolment process.