|  |
| --- |
| Input Contribution |
| Meeting ID\* | SEC 31 |
| Title:\* | Use Case 1 - Verify IoT Application identity and integrity |
| 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 : Verify IoT Application identity and integrity

### 5.x.1 Description

IoT applications can enter into the supply chain via many routes. With the best intentions it is not possible to 100% secure the control of the supply chain though manufacturers, distributors, resellers, 3rd party contractors and consumers.

Many IoT service are required to provide open access for unknown IoT applications to connect, for example smart homes, cities, healthcare. The economies of these services are built upon consumers and businesses being able to acquire their own IoT applications and connect them with these smart communities.

Even when IoT systems are vertically integrated, such as industrial controls, factories, utilities etc, the IoT service provider will find it difficult to control the supply chain and cannot guarantee 100% that all the IoT applications are authentic.

Where this happens at scale for example 1000’s IoT sensors with an industrial deployment or a smart city needing to authenticate various brands makes and models of connected vehicles. Scale exacerbates the problem for supply chain controls.

**Using App-ID Registry Function to provide IoT identity and integrity checking.**

A Service provider Infrastructure can verify the identity of a connecting IoT application by connecting with the App-ID Registry Function. A 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. The App-ID metadata can contain the following attributes to allow the SP be informed to make decisions how to allow the IoT application connect, if at all :-

* **IoT application Type:** Information regarding the type of application, for example thermostat, vehicle telemetry, or fan control.
* **IoT application Class:** Details for the class of use: consumer, industrial, or critical infrastructure. The~~se~~ class type will have a bearing on how the data and security of the IoT application is enrolled onto the SP.
* **Security capability**: The security capabilities of the IoT application. This will indicate the security capabilities of the IoT application, authentication, as well as the ability for the IoT application to secure a private key in a trust enclave.
* **Authentication type:** The mechanism ~~is~~ used to authenticate the IoT Application. For example, if using a PKI certificate, who is the root of trust.
* **Communications class:** The profile for the data generated by the application. For example, streamed data, periodic burst of data, or intermittent bursts of data.
* **Data Model:** The data definition for the application, what is projected, and the actions that can be performed. The application data model and mapping to oneM2M ontology.
* **Data privacy:** The data privacy asserted for this App-ID. The generic data privacy model for the application identity. For example, the IoT application is a blood pressure monitor and the data can only be provided to the client’s electronic health record. The data cannot be shared, data mined, or resold by the IoT service provider

Using the App-ID metadata provided by theApp-ID Registry Function, the SP can verify the identity and authenticity of the connecting IoT application. Also it can assign the right resources for the connecting IoT application

This functionality will allow any registered App-ID to provide an application profile in form of metadata that can be used by a SP to identify and verify that the connecting IoT application is representing itself consistently with the characterization presented by the metadata.

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