1

2

3

INPUT CONTRIBUTION	
Meeting ID*	TP-18 (Philadelphia)
Title:*	TIA Input on Application ID and Related Issues
Source:*	David Crowe, IFAST, +1-403-289-6609, David.Crowe@ifast.org
	Mihai Voicu, ILS Technology,+1-561-214-4559, mvoicu@ilstechnology.com
	Richard Brennan, Telxxis, +1 510-895-9852, rbrennan@telxxis.com
Uploaded Date:*	2015-MM-DD
Document(s) Impacted*	TS0001, TS0011
Intended purpose of document:*	☒ Decision ☐ Discussion ☐ Information ☐ Other <specify>
Decision requested or recommendation:*	Review the background provided on Application ID and related issues in TS0001, TS0004 and TS0011 and make the recommended changes to TS0001 and TS0011 (no changes to TS0004 are recommended).
Template Version:23 February 2015 (Dot not modify)	

4

oneM2M Notice

5

6 The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any
7 activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the
8 Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in
9 Annex 1 of the Partnership Agreement.

10

11

1 Introduction

These ballot comments are related to the App-ID concept in oneM2M specifications.

Background

Some relevant portions of specification text relating to App-ID (and M2M applications in general) are:

TS 0001

- (7.1.3) "An Application Identifier (App-ID) uniquely identifies an M2M Application in a given context. More precisely, there are two types of App-ID: registration authority defined App-ID (registered App-ID) and non-registered App-ID. The establishment of the registered App-ID is guaranteed to be globally unique; the non-registered App-ID is not guaranteed to be globally unique."

- (7.2) App-ID is defined as: "Either "R[authority-ID]/[registered-App-ID]" or "N[non-registered-App-ID]" If the first letter is "R", then authority-ID and registered-App-ID are assigned by the registration authority. The registered-App-ID is managed by the owner of authority-ID. If the first letter is "N", then non-registered-App-ID is not registered by the registration authority."

- (9.6.1.1) "serviceSubscribedAppRule – Represents a rule that defines allowed App-ID and AE-ID combinations that are acceptable for registering an AE on a Registrar CSE"

- (9.6.29) "List of App-IDs that shall be considered to be allowed for AE registration requests received via Security Association Endpoint (SEA) [i.3] associated with credentialID stored in the attribute applicableCredID. This can contain '*' for any App-ID. Also Wildcards within an element of this list are possible (e.g. 'C123*X' for any App-ID that starts with 'C123' and ends with 'X') to define sets or ranges of App-IDs."

- (11.2.2) "[M2M Application Enrollment] assumes that M2M applications obtains or registers credentials to be used for controlling authorization with an M2M application registration authority (see clause 7.1.3). Each application identified by an App-ID is then associated with a security credential (M2M Application key) which can be used to grant specific authorization to access an approved list of M2M services. Such authorization takes place between a CSE and an AE as specified in the present document and the oneM2M Security Solutions Technical Specification".

TS 0004

- (7.3.5) App-ID is defined as an attribute of the AE resource.

TS 0011

- (3.2) "M2M application: applications that run the service logic and use M2M Common Services accessible via a set of oneM2M specified open interfaces. NOTE: Specification of M2M Applications is not subject of the current oneM2M specifications.."

M2M Application

The definition of "M2M Application" in TS0011 does not clarify whether the term "M2M application" is restricted to the field domain, or whether it also encompasses applications in the network domain. Importantly, it does not address whether a single "M2M application" can span both domains.

This directly impacts the usage of App-IDs, particularly in what might be considered distributed applications, with software resident in both the field domain and network domain. The use of a single App-ID to identify software in both domains may introduce complexities and ambiguities and so is not recommended.

The main question is whether an application in the network domain can qualify as an "M2M application" and therefore whether they can be identified by an App-ID. Most of the App-ID discussions reference the CSE and AE (field domain).

Recommendations (TS0011)

Add one of the following statements to the definition of "M2M Application" in TS 0011:

- The term M2M application is restricted to the field domain. OR

- An M2M application may exist in the field domain, or the network domain, but not both.

Application ID Format

The application ID currently has the following components:

- Authority letter. "R" for registered, "N" for non-registered.
- Authority ID (for registered App-IDs only)
- App-ID

A concern with this is:

- The inclusion of the registration authority ID makes identifier portability more difficult. It implies that queries for Application ID must go to a specific registrar, but this is not necessary even if there are multiple registrars (all registrars could synchronize their data, for example). It may be worthwhile considering removing the Authority ID from the format.

Recommendations (TS0001)

Modify the App-ID format definition as indicated by the change marks:

- Either "R [authority-ID]/[registered-App-ID]" or "N[non-registered-App-ID]" If the first letter is "R", then the authority-ID and registered-App-ID are is assigned and managed by the registration authority. The registered-App-ID is managed by the owner of authority-ID. If the first letter is "N", then the non-registered-App-ID is not registered by the a registration authority.

M2M Application Key

The M2M Application Key is mentioned in only one place, in TS0001, "[M2M Application Enrollment] assumes that M2M applications obtains or registers credentials to be used for controlling authorization with an M2M application registration authority (see clause 7.1.3). Each application identified by an App-ID is then associated with a security credential (M2M Application key) which can be used to grant specific authorization to access an approved list of M2M services. Such authorization takes place between a CSE and an AE as specified in the present document and the oneM2M Security Solutions Technical Specification".

Without any details it is unclear what kind of key this is and whether it is unique for the application, or for each instance of the application. It implies that this is obtained from the application registry, but it is not clear how the "M2M application key" will be derived with the assistance of the registry. Nor is it clear how a key can be used to "grant specific authorization to access an approved list of M2M services".

Recommendations (TS0001)

The purpose, structure and usage of the "M2M Application Key" should either be greatly expanded or mention of this should be removed from TS 0001. If this is done the entire section 1.2.2 may have to be removed.

Data Associated with App-ID

If it is possible to query a registry for an App-ID, at least the minimal information that will be returned should be defined. This is not in any specification, but was proposed in an ATIS/iConectiv contribution to the App ID ad hoc group. Since the contribution was not accepted, it is not discussed here.

Organizations that can obtain the information should also be defined, but this is probably more appropriate by industry assignment guidelines rather than in a specification.

Recommendations (TS0001)

Define the information associated with an App-ID:

- App-ID

- Assignee

- Application Description

- Registrar

- Date of assignment

- Current status (e.g. Pending Assignment, Assigned, Being Withdrawn)

Note that we do not include the software version (which was in the ATIS/iConectiv contribution), because we assume that an App-ID is valid for every software version, unless the software publisher believes that a new version is different enough that a separate ID is required.