

Welcome to the World of Standards



Take away and open issues

2nd DG CONNECT & ETSI Workshop on Smart Appliances,
14 October 2014

Is ETSI M2M/oneM2M solution compatible with the SMARTGRID requirements defined by ETSI/CEN/CENELEC?

- In the case of the SMARTGRID case there is a requirement related to strict real time control with very high figures. These numbers that are not even reachable with current communication IP, cellular or fixed networks. ETSI M2M and oneM2M are IP based and are reusing web based approaches that are currently not compatible with this high figures. Anyhow information about the energy use can be collected and reused as big data.

About study group approach and documentation

- The common ontology needs to be appropriately detailed to allow the transformation of the study into a specification and to cater for the mapping on the basic ETSI M2M/oneM2M objects. More common meeting and an early share of information among the Study group team and ETSI M2M is envisage (directly or via Study group representative).
- The approach taken is looking at a bottom-up approach. Another option to explore is the reuse of existing ontologies approaches, to facilitate the worldwide use of the Smart Appliances specification.

ETSI Test specifications:

- ETSI M2M is going to define test specification for the ontology and the communication system, ETSI will also provide occasions for plug-test events to facilitate development of interoperable solution. ETSI WILL NOT perform tests for certification purposes. It is expected that the manufacturers of the smart appliances will certify their products, directly or via third parties.
- ETSI is currently planning to test specification for the common ontology together with the communication system. It is possible to study the testing of the common ontology standalone, but this is not currently planned

Security in ETSI M2M / oneM2M

- The security and privacy requirements are in the corresponding stage 1 specification of ETSI M2M (TS 102 689) and oneM2M (TS-0002-Requirements). Anyhow the approach taken can be better understood reading the security section of ETSI M2M specification (TS 102 689) and the Access Right resource management (or their corresponding counterparts in oneM2M)

Study group report:

- Regarding the Smart 2013/007 second report, inside HGI we are looking at three levels of information that might be considered , and which may not all be desirable in all cases: (a) manufacturer information about what a device can do (b) real-time data generated by a device (c) user-generated content telling the context. The example is (a) here is a thermometer that can measure in Celsius (b) here is the temperature at the current time (c) actually it is the temperature in the fish tank in my home. The work from TNO in Smart 2013/007 is concentrating on (a) and (b).
Security in ETSI M2M / oneM2M

Collaboration with CENELEC:

- CENELEC has some extremely valuable work in TC205 WG18 on semantics, however I understand it cannot be shared directly with ETSI due to organizational rules. I hope that the EC can find a way to ensure wide cooperation?