Comments on IEEE P802.15.9a CSD

From IEEE 802.1

These comments are on the CSD found in:

- https://mentor.ieee.org/802.15/dcn/24/15-24-0286-02-cryp-csd-for-tg9a.docx

CSD

1.2.1 b) Broad Market Potential

- Consider revising to:

  “

  IEEE Std 802.15.9 was designed to include multiple key management protocols, so different environments could select a suitable key management protocol for their use case. One of the challenges with existing KMPs is that all of them use messages that require fragmentation in a typical IEEE 802.15.4 PHY. EDHOC has a mode of operation where each message is less than 50 bytes, meaning it does not need fragmentation.

  There are multiple silicon and system vendors producing devices and systems using IEEE Std 802.15.4 in combination with IEEE Std 802.15.9 for use in IoT applications. This includes consumer electronics, mobile devices, building automation, medical applications, SmartGrid and Smart Community applications, industrial control, etc., and therefore has a very large end user community.

  “

CSD

1.2.2 Compatibility

- Suggest moving answer currently at the bottom to under 1.2.2 a)
- Suggesting adding to the bottom:

  "This project is an amendment to an existing standard for which it has been previously determined that compliance with IEEE Std 802.1Q is not possible. The project will comply with IEEE Std 802 using either local or global MAC addresses."

CSD

1.2.3 Distinct Identity

- Consider revising sentence 1 to:

  “IEEE Std 802.15.9 was developed specifically to allow multiple KMPs, so each environment can select one for its needs.”

CSD

1.2.5 Economic Feasibility

- Consider revising to:

> “EDHOC allows smaller message sizes than any other KMP in IEEE Std 802.15.9. The cost of the implementation should be same in coordinators and devices, and there is no special installation or operational costs. “