Comments on IEEE P802.15.4ae CSD

From IEEE 802.1

These comments are on the CSD found in:

- https://mentor.ieee.org/802.15/dcn/24/15-24-0268-01-cryp-csd-for-tg4ae.docx

CSD

1.2.1 Broad market potential b)

- Suggest changing last sentence in first paragraph to: “NIST selected the Ascon algorithms as its lightweight cryptographic standard, making its use in the future more widespread.”
- Suggest Removing "things like" in the second paragraph.

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

- Suggest revising paragraph to:

  “IEEE Std 802.15.4 was developed to address the needs of IoT networks and is used in those areas. Adding Ascon-128 and/or Ascon-128a to the standard will allow devices to use more lightweight cryptographic algorithms. Ascon-128 and Ascon-128a offer functionality not available in AES, like hashing and key material extraction, so it can be used in more cases than AES.”

CSD

1.2.4 Technical Feasibility

- Suggest revising paragraph to:

> “Ascon was announced as winner of the NIST's lightweight cryptographic standard competition. During the competition it received a large number of third party reviews, and verifications. There are multiple existing implementations of it.
>
> It uses the same AEAD framework as used in the IEEE Std 802.15.4, thus dropping it in to the existing IEEE Std 802.15.4 security framework should be straightforward.
>
> ”

CSD

1.2.5 Economic Feasibility

- Suggest fixing spellings of “implementation”.

- Are there also operational cost savings as a result of a smaller footprint? If so, consider noting.