Dear Colleagues,


In this draft, a number of items are identified as truly optional MAY; it would appear that some of these items would override restrictions in other security standards. For example, in Section 3, Support for Built-in Keys, there is discussion about copying the built-in keys; however this is restricted by IEEE Std 802.1AR. The draft should be clear that where provisions of referenced security standards appear to conflict or restrict the operations described in the draft, those other security standards take precedence.

The certificate encoding specified does not appear to use any standard encoding (e.g., DER/BER). It also might be useful to reference a standard key wrap or specifier for a standard key wrap algorithm for transporting both symmetric and asymmetric keys.

There is an updated standard IEEE Std 802.1AR, *Secure Device Identity*, which is IEEE Std 802.1AR-2018. And there are extraneous letters (i.e., Group, W. -. H. L. L. P. W.) in the reference for [Std-802.1AR-2009] which should be removed.

Thank you for your consideration on this topic. We look forward to continued collaboration and discussion between our organizations.

Respectfully submitted,
Glenn Parsons
Chair, IEEE 802.1 Working Group