

Title: Liaison on a YANG Data Model for a Keystore  
From: IEEE 802.1 Working Group  
For: Action  
Contacts: Glenn Parsons, Chair, IEEE 802.1, [glenn.parsons@ericsson.com](mailto:glenn.parsons@ericsson.com)  
Jessy Rouyer, Vice-Chair, IEEE 802.1, [jessy.rouyer@nokia.com](mailto:jessy.rouyer@nokia.com)  
Mick Seaman, Chair, IEEE 802.1 Security Task Group, [mickseaman@gmail.com](mailto:mickseaman@gmail.com)  
To: Lars Eggert, Chair IETF, [lars@eggert.org](mailto:lars@eggert.org)  
IETF Liaisons, [statements@ietf.org](mailto:statements@ietf.org)  
Copy: Paul Nikolich, Chair, IEEE 802, [p.nikolich@ieee.org](mailto:p.nikolich@ieee.org)  
Karen Randall, Liaison Secretary, IEEE 802.1, [karen@randall-consulting.com](mailto:karen@randall-consulting.com)  
Jodi Haasz, Manager, IEEE SA Operational Program Management, [j.haasz@ieee.org](mailto:j.haasz@ieee.org)  
Russ Housley, IETF/IEEE 802 Coordination Chair, [housley@vigilsec.com](mailto:housley@vigilsec.com)  
Dorothy Stanley, IEEE 802/IETF SC Chair, [dorothy.stanley@hpe.com](mailto:dorothy.stanley@hpe.com)  
Date: 6 October 2021

Dear Colleagues,

The IEEE 802.1 Security Task Group reviewed the Internet-Draft *A YANG Data Model for a Keystore* (<https://datatracker.ietf.org/doc/draft-ietf-netconf-keystore/>).

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 of these matters, and we welcome continued collaboration going forward.

Respectfully submitted,  
Glenn Parsons  
Chair, IEEE 802.1 Working Group