

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: Alissa Cooper, Chair IETF, [alissa@cooperw.in](mailto:alissa@cooperw.in)  
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: 23 September 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/>).

The IEEE 802.1 Security TG has concerns that IEEE Std 802.1AR, *Secure Device Identity*, is not accurately described. In 3, Support for Built-in Keys, there is discussion about copying the built-in keys; however this is not permitted by IEEE Std 802.1AR because it can introduce a security weakness or expose the DevID secrets. The certificate encoding specified does not appear to use any standard encoding (e.g., DER/BER). There is also no reference to TPM (Trusted Platform Module) for a secure hardware platform.

Furthermore, 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