Title: Liaison response to Liaison Statement to IEEE 802.1 – Secure Device Onboarding using WBA OpenRoaming
From: IEEE 802.1 Working Group
For: Information
Contacts: Glenn Parsons, Chair, IEEE 802.1, glenn.parsons@ericsson.com
Jessy Rouyer, Vice-Chair, IEEE 802.1, jessy.rouyer@nokia.com
Mick Seaman, Chair, IEEE 802.1 Security Task Group, mickseaman@gmail.com
Paul Nikolich, Chair, IEEE 802, p.nikolich@ieee.org
Karen Randall, Liaison Secretary, IEEE 802.1, karen@randall-consulting.com
Jodi Haasz, Manager, IEEE SA Operational Program Management, j.haasz@ieee.org
To: Bruno Tomas, Director, Wireless Broadband Alliance, bruno@wballiance.com
Mark Grayson, OpenRoaming TG, WBA, mgrayson@cisco.com
Betty Cockrell, OpenRoaming TG, WBA, bcockrell@singledigits.com
Finbarr Coghlan, OpenRoaming TG, WBA, finbarr.coghlan.ext@orange.com
Necati Canpolat, OpenRoaming TG, WBA, necati.canpolat@intel.com
WBA PMO, pmo@wballiance.com
Date: March 16, 2021

Dear Colleagues,

The IEEE 802.1 Working Group would like to thank Wireless Broadband Alliance for the information provided in the Liaison Statement about Secure Device Onboarding using WBA OpenRoaming.

As your Liaison Statement points out, Annex B of IEEE Std 802.1AR-2018 describes a device that uses a DevID in an EAP-TLS exchange. IEEE Std 802.1AR references the use of IETF RFC 7030 (Enrollment over Secure Transport, EST) and references the draft Bootstrapping Remote Security Key Infrastructures (BRSKI) for enrollment exchanges.

For device enrollment into a roaming federation service, it may be possible to use EST which describes a Public Key Infrastructure (PKI) certificate enrollment for client certificates (and associated Certification Authority (CA) certificates) using Crypto Message Syntax (CMS) messages over a secure transport. Additionally, the draft of BRSKI describes protocols and a framework for an automated enrollment information exchange using manufacturer installed certificates (e.g., the IDevID defined in IEEE Std 802.1AR) to deploy or install a new cryptographic identity to a device. BRSKI has been under development in the ANIMA WG in IETF and is currently awaiting publication.

We look forward to further communication and welcome any contribution you may have on the subject.

Note that the IEEE 802 work is open and contribution driven. Participation is on an individual basis and technical discussion can be conducted based on individual contributions. The Security Task Group holds regular electronic meetings: details are available at https://1.ieee802.org/wg-calendar.

Respectfully submitted,
Glenn Parsons
Chair, IEEE 802.1 Working Group