| | |
|---|---|
| **Date** | 15 January 2021 |
| **WG / Project** | WBA OpenRoaming Standards Group |
| **To** | Jodi Haasz – IEEE Program Manager - j.haasz@ieee.org<br>Glen Parsons, Chair 802.1 WG - glenn.parsons@ericsson.com<br>Mick Seaman, Security TG Chair - mickseaman@gmail.com |
| **OpenRoaming TG chaired by** | Mark Grayson (Cisco)<br>Betty Cockrell (Single Digits)<br>Finbarr Coghlan (Orange IC)<br>Necati Canpolat (Intel) |
| **Topic** | Secure Device Onboarding using WBA OpenRoaming |
| **Action ID Prefix** | N/A |

## Dear IEEE 802.1

The Wireless Broadband Alliance (WBA) is committed to accelerate the adoption of secure onboarding of Wi-Fi devices and roaming. As part of this endeavor, WBA has developed the OpenRoaming federation service enabling an automatic and secure Wi-Fi experience globally. With WBA OpenRoaming$^{TM}$, WBA has created an open connectivity framework for all organizations in the wireless ecosystem to power new opportunities in the 5G era.

OpenRoaming encompasses three key elements:

- **Cloud federation:** creates a federation of access networks and identity providers to enable automatic roaming and user onboarding on Wi-Fi. Based on WBA's Wireless Roaming Intermediary eXchange (WRIX) standards to scale and facilitate different business models under a harmonized framework.
- **Cyber Security:** enables simple, secure and scalable Wi-Fi connections amongst different organizations that are part of WBA OpenRoaming. Allowing automatic and secure roaming between millions of networks, nationally and globally with secured interconnection and encrypted communications that are used to authenticate end-devices using a Passpoint/EAP exchange.
- **Network automation:** defines an automated roaming consortium (RCOI) codes framework to support policy provision on devices and networks. Organizations that manage a Wi-Fi CERTIFIED Passpoint enabled network may become part of the OpenRoaming federation.

OpenRoaming is targeted at accelerating the adoption of conventional settlement-based services, but is also able to accelerate the adoption of settlement-free use cases. In particular, the settlement-free capability has opened up the range of identity providers involved with Wi-Fi roaming. For example, already Pixel and Samsung smartphones now come pre-installed with settlement-free OpenRoaming profiles that leverage roaming using Google-ID and Samsung-ID respectively.

OpenRoaming scales by using DNS to enable the automatic discovery of an OpenRoaming Identity Provider (IDP) by an OpenRoaming Access Network Provider (ANP) based on the realm recovered from the Network Access Identifier (NAI) provided by the roaming device in its EAP-Response/Identity message. The WBA PKI enables the subsequent signaling between the ANP and IDP to be secured with PKI-RadSec established using certificate-based mutual authentication.

Outside of the conventional smartphone use-cases, WBA is already engaging with a number of Wi-Fi device manufacturers that are investigating how they can leverage the OpenRoaming federation for their onboarding requirements, e.g., using manufacturer installed certificates and an EAP-TLS exchange.

WBA notes that IEEE 802.1AR-2018 already describes the use Secure Device Identifiers in combination with an EAP-TLS exchange. WBA would like to facilitate the use of the OpenRoaming federation for onboarding devices with initial DevID certificates. The scenario envisaged is where the supplier or manufacturer of the device offers a publicly accessible EAP-TLS authentication service when operating as an OpenRoaming Identity Provider. Such a capability enables the supplier or manufacturer to on-board its devices onto third party networks (OpenRoaming Access Networks) while using a private certificate authority to issue the initial DevID certificates.

## Specific request

When comparing IEEE 802.1AR-2018, specifically the existing DevID certificate and informative EAP-TLS annex, with the capabilities necessary for enabling secure device on-boarding using OpenRoaming, the aspect not clearly defined relates to ensuring that a realm can be signalled in the EAP-Response/Identity to enable the automatic discovery of manufacturer’s RadSec server. One approach could be to define how a manufacturer’s realm can be optionally configured in the DevID certificate subject field and how a device’s supplicant can use such in creating its EAP-identity.

WBA would welcome the opportunity to work with IEEE 802.1 to understand how best to enable the use of the OpenRoaming federation for enabling the automatic onboarding of IEEE 802.1AR devices onto OpenRoaming Access Networks.

For any additional information, please contact the WBA PMO at pmo@wballiance.com.

Thank you,

WBA PMO

**Next WBA Meetings:**

**2021 Q1 Virtual Working Sessions – February 2-4**

**2021 Q2 Hybrid Working Sessions – Jun 14-17**

Learn more here - https://www.wirelessglobalcongress.com/