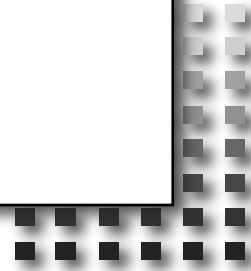




IETF Hackathon: EAPRAD

**IETF 121
2–3 November 2024
Dublin, Ireland**



Hackathon Plan

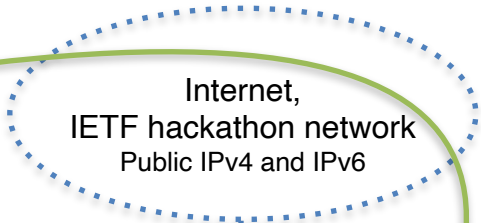
- EAP-FIDO implementation work
 - emu working group: <https://datatracker.ietf.org/wg/emu/about/>
 - <https://datatracker.ietf.org/doc/draft-ietf-emu-eap-fido/>
- Discussing RADIUS drafts currently in the radext working group, trialling and testing implementations
 - radext working group: <https://datatracker.ietf.org/wg/radext/about/>
 - RADIUS over TLS (RadSec) update: <https://datatracker.ietf.org/doc/draft-ietf-radext-radiusdtls-bis/>
 - RADIUS and TLS-PSK: <https://datatracker.ietf.org/doc/draft-ietf-radext-tls-psk/>
 - Deprecating Insecure Practices in RADIUS: <https://datatracker.ietf.org/doc/draft-ietf-radext-deprecating-radius/>
- RADIUS over TLS (RadSec) interoperability testing with Aruba, Meraki and Ubiquiti hardware focusing on the configuration of the RADIUS over TLS details, certificate validation, TLSv1.3 support
- OpenRoaming roaming test network setup utilizing RADIUS over TLS (RadSec) connections and multiple IdP profiles including SIM authentication with dynamic 3GPP realm/IdP discovery

**OpenRoaming
Access Network Provider (ANP)**

RadSec Server



RADIUS over TLS
Connections from APs
To ANP server

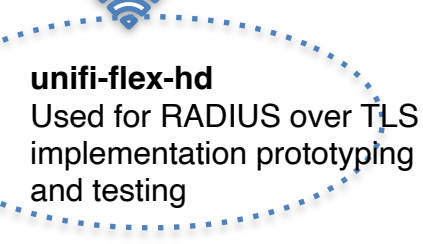
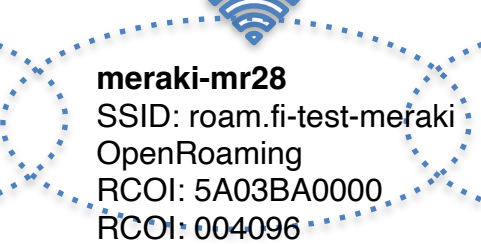
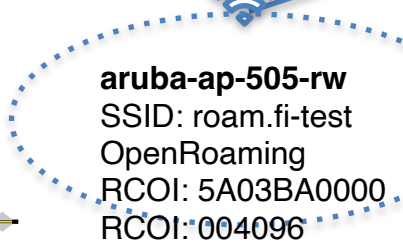


asus-rt-ax59u
OpenWRT 23.05

Successful bonus test:
DHCPv6 Prefix Delegation
NATed IPv4, Public IPv6 LAN
With default OpenWRT configuration


















unifi-sw-lite-8



I E T F

AP RadSec implementation testing



	Ubiquiti FlexHD	Meraki MR28	Aruba APIN0505
Configuration interface			
Server address	Literal IPv4 only 	Literal IPv4/6, or FQDN 	Literal IPv4/6, FQDN 
Shared secret	No default 	No default 	Default per RFC 
Certificates	User provided 	Server CA: user provided Client CA: given by Meraki 	User provided 
TLS connection			
TLS version support	1.3 	1.2 	1.2 
Server identity validation			

*actual connections only tested over IPv4

OpenRoaming IdP tests

- Successful roaming with at least 5 different OpenRoaming IdPs
- Successful roaming with SIM authentication utilizing DNS discovery for finding IdP server based on the mnc.mcc.3gppnetwork.org realm

What we learned

- RADIUS over TLSv1.3 support is not yet at least these tested access point with the latest stable and beta software.
- Certificate installation, handling, validation and configuration needs improvements in all of the tested access points.
- Comments about drafts will be presented in the respective working groups.

Wrap Up

Team members:

Jan-Frederik Rieckers

Karri Huhtanen

Heikki Vatiainen

Fabian Mauchle

Alex Clouter

Subir Das

Alan DeKok