IETF 89 - opsawg meeting
London, 04 Mar 2014

draft-winter-opsawg-eap-metadata
Why this work?

- IETF has produced a great standard for authentication: Extensible Authentication Protocol
- EAP is a mere container, carries EAP Methods
  - Needs some configuration itself (e.g. max fragment size)
- Each method has its own set of configuration parameters
  - Authenticate EAP server to the EAP peer
  - Authenticate EAP peer to the server
  - Anonymity support
  - … and plentiful more
- Multiple methods can be configured; priority?
So?

- EAP server setup must match EAP peer's configuration for successful auth.
- EAP peers are configured by **end users** (argh!)
  - Lengthy PDF instructions are the norm, especially in BYOD.
  - EAP peer UIs typically make it easier to be insecure than secure (« Don't validate server certificate » ; « do you trust this fingerprint ? »)
- The best auth protocol can't deliver if its users get it wrong.
Existing Approaches

- For some operating systems, EAP peer software accepts (proprietary) config files with some/all the right settings
  - Apple « mobileconfig »
  - Microsoft « netsh XML profile »
  - Intel « PRO/Set Wireless »
  - Wi-Fi Alliance Hotspot 2.0 « Per-Provider Subscription Managed Object »

- All of those duplicated work, and delivered partial solutions (need war stories?), none of which interop
This draft – Overview

- Fill the void: IETF has produced EAP – so it should also produce a sensible deployment option
- De-duplicate per-vendor approaches
- Produce actual implementations
  - We have three:
    - XML producer (alpha, unreleased module for https://cat.eduroam.org)
    - XML consumer: Linux (prototype, uses D-Bus to push settings to EAP peer software wpa_supplicant)
    - XML consumer: Android app (prototype, needs API level 18+)
This draft – Technical

• Using XML Schema
  • because it's popular and straightforward
  • Subject to discussion: YANG? JSON?

• XML contains
  • Technical EAP settings (CA, server name, anon ID allowed?, optional pre-load with username/password, EAP method chaining ...)
  • Meta-Info: name of the organisation which provides access credential, org logo, Terms of Use, etc.

• Does not contain WiFi-specific settings (topic in hands of IEEE; and EAP is not just about WiFi anyway) – unique identifier in the file to enable cross-referencing from e.g. a WiFi configuration spec
Future Plan

• Hope to adopt draft as WG item in opsawg
  • No other WG is spot-on
    • emu – only about methods, and also closing down
    • radext – much of EAP goes over RADIUS, but RADIUS doesn't care about the payload
    • dime – same situation as RADIUS
  • opsawg was suggested path from OPS ADs
• If adopted, aiming for STD track