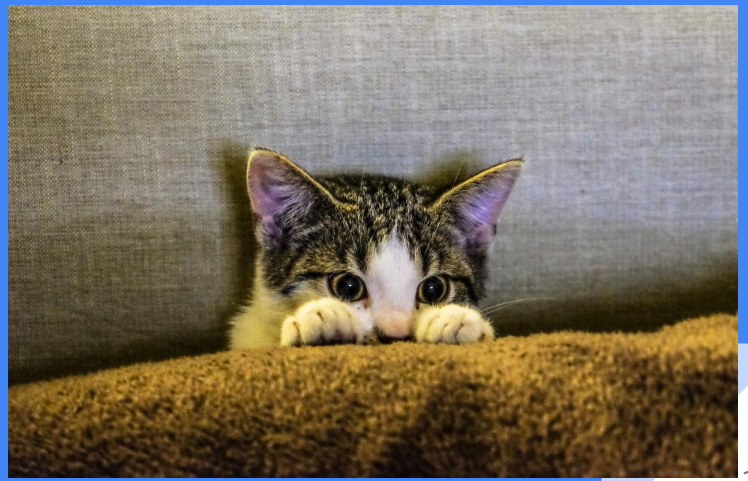
Moving from .1X to WPA2/3

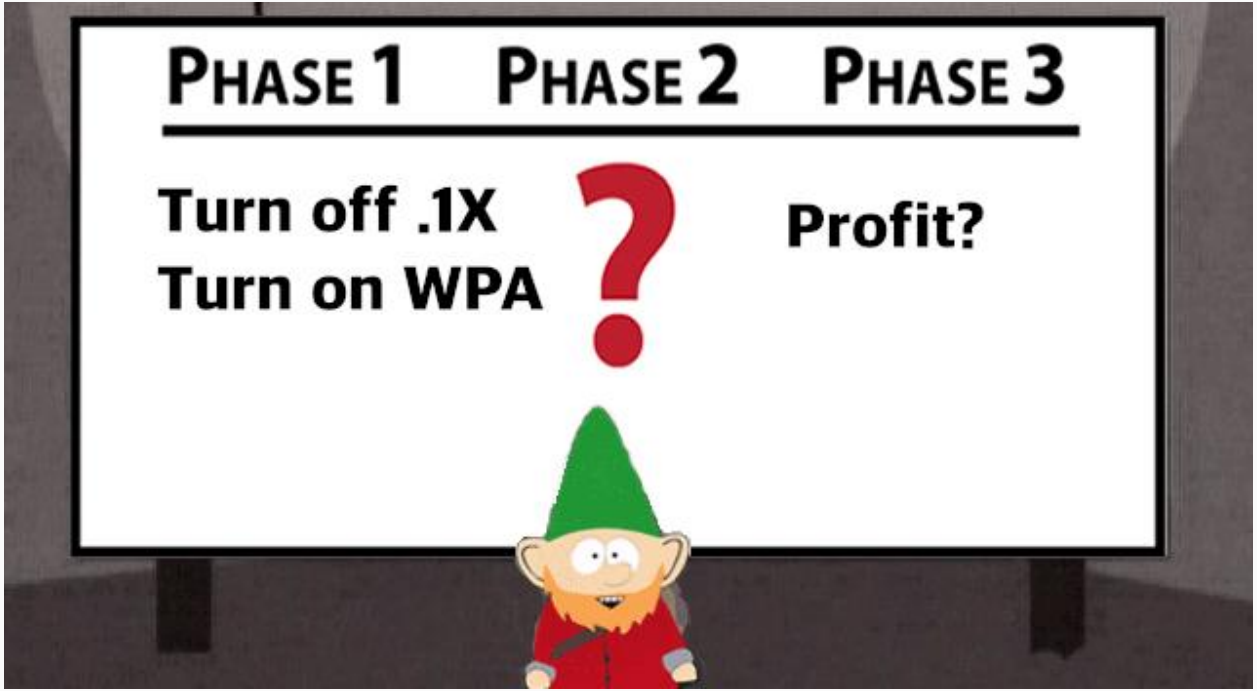
Because it’s super good enough…



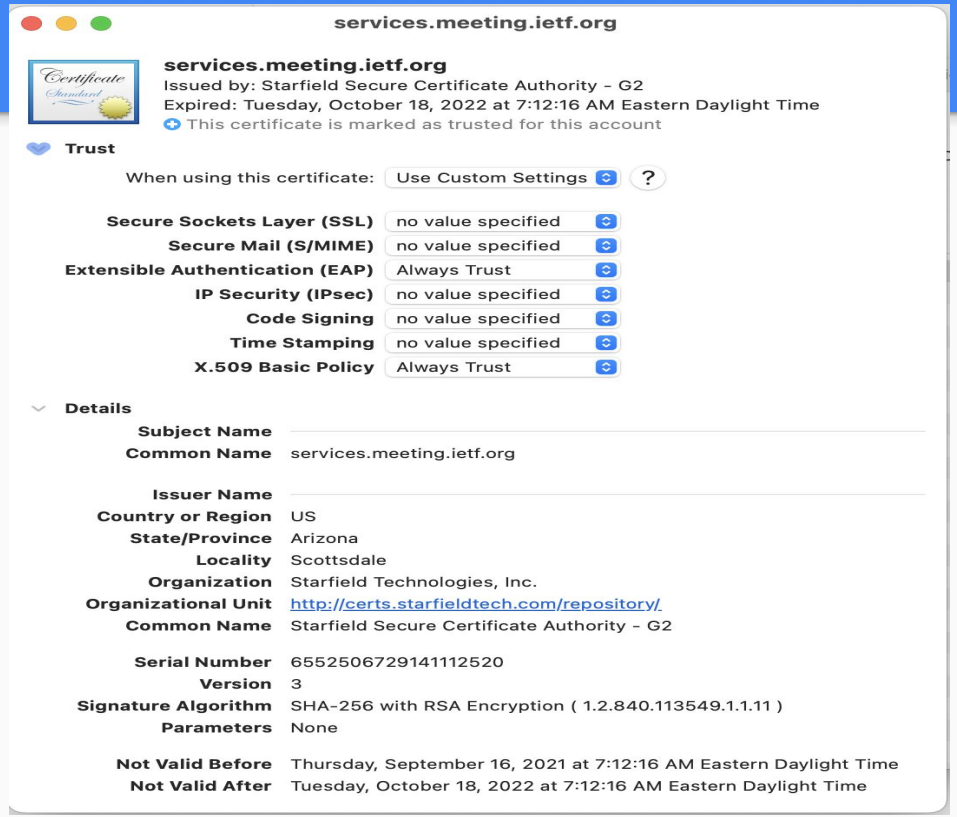
Pedant Appeasement

- **When I say “802.1X” I mean “WPA2-Enterprise using EAP-Protected EAP (which uses TLS & certificates to create a tunnel to the authentication server), and an inner EAP method of MSCHAPv2 to perform the user authentication against a RADIUS server”…**
  - **… “dot1x” is just easier to say :-)**

The plan! The plan!!!



Certificates make users sad…



If it ain’t broke, why are you touching it?!

- **People blindly trust the new certificate, negating any security benefit**
  - **We used to have https://802.1x-config.org/?idp=137&profile=101, but:**
    - **1: No one used it…**
    - **2: … and it’s gone!**
  - **Cert fingerprint is posted on the meeting page, but no one uses it[0]**
  - **Approximately 1 in 3 meetings the cert changes (1 year validity, 3 meetings)**
- **No authority to install certificates on managed devices**
- **Complexity of cert installation on various OS**
- **Proof? Helpdesk gets 2-3 tickets per day related to this**

[0]:For at least one meeting, the fingerprint was wrong, and no-one noticed!

Android Configuration

A Note For Android Users

Here are the relevant settings for connecting Android devices to the secure ietf networks.

- Network name (*e.g.* ietf): **ietf**
- Security: **WPA/WPA2-Enterprise**
- EAP Method: **PEAP**
- Phase 2 authentication: **MSCHAPv2**
- CA Certificate: **Use system certificates**
- **Do not verify**
- Domain: **services.meeting.ietf.org**
- Identity: **ietf**
- Password: **ietf**

If this is so bad, why did we start?!

- WEP -> WPA -> WPA2 -> WPA3…
  - NOC team believes WPA3 is super good enough, and WPA2 is good enough.
  - We believe (perhaps wrongly!) that deployment of encrypted Layer-3 (e.g TLS) has reached the point that if one is breached, another is still in place.
    - E.g: people are comfortable using ietf-hotel and coffee shops, etc.

- Evil Twin Attack
  - … but no-one checks the certs anyway, so .1X didn't fix that.

- Potential flexibility
  - Ability to put people in special networks based on their credentials.
  - Never used this, so… ¯_(ツ)_/¯

FAQ

- If everyone uses the same WPA2 PSK, can't anyone sniff the traffic?
  - Nope. PSK is used to derive Pairwise Transport Keys. This is (conceptually) similar to how we all use "ietf"/"ietf" currently.
- … but someone who can see the 4-way handshake could derive the PTK! Mwahahaha!
  - Yes. A local attacker who can see both sides can indeed derive the WPA2 PTK - but is this really a threat you are concerned about? These days, almost all networks are either open (the airport / coffee shop) or use WPA. Also, see "ietf-hotel". This is why we have TLS and other layers of security
- Why don't you only do WPA3? It's the new hotness!
  - Yes, yes it is. Unfortunately many devices don't support it yet. If yours does, yay, you'll use the WPA3 capability. If yours doesn't, WPA2 is good 'nuff.

Feedback…

We are likely out of time, so let’s take this offline…

Impact to NOC of staying on .1X

- **Additional Infrastructure - RADIUS**
  - **Will still need this for EduRoam, but it's not in the critical path for "ietf" network**
- **Additional help-desk tickets**
  - **See next slide!**
- **Additional toil (renewing the 802.1X certificate)**
  - **This sounds like it should be easy, but reasons…**

Certificates

From the network announcement mail:

All networks marked as encrypted provide layer 2 security. They use WPA2 Enterprise with 802.1X (PEAP or TTLS) authentication and AES encryption. Although all users are using the same credentials (user **'ietf'**, password **'ietf'**), each user gets unique session encryption keys. The certificate for services.meeting.ietf.org is signed by Starfield Technologies, Inc., with the following fingerprint.

hash f(x)	**fingerprint**
SHA1	DB:2A:E7:D1:AF:B5:5A:03:43:11:BC:B0:AD:77:E9:D1:D7:12:A7:25
SHA256	8A:AC:ED:35:86:7F:FC:35:C2:82:33:AA:E4:6A:CA:C5:8E:97:20:9C:6D:73:82:9E:CB:26:77:D6:A4:72:A9:C5

IETF 115 - London

As we renew our certificate for the 802.1X authentication every year, the certificate has been updated between IETF 114 and IETF 115. The NOC team has discovered that some devices with an existing profile for an IETF SSID (e.g., ietf) with the old certificate have a network association problem. This is most noticeable on Apple iOS devices. You may get an “unable to join the network” error message on your device if you have this problem.

If you have a problem associating with any 802.1X-based IETF SSIDs, the solution is to forget the SSID/network from your device and then try to associate with it again. If you need assistance please visit the help desk.