Identities

IN EAP TYPES
ALAN DEKOK IETF 106
WHAT DO TO?

- Some discussion (my long comments don’t appear in the EMU WG list archive)
- Summary: recommend using @realm
  - Everywhere, for all EAP types, all of the time.
  - other systems MAY be used, but will not be compatible with roaming
At a high level, an authentication request can contain multiple identities at different layers:

- User-Name (RADIUS / Diameter)
- EAP Identity (EAP)
- PSK Identity / certificate common name (TLS)

These identities are commonly the same, but they don't have to be. So the question is which identity to use where.

We can say that EAP Identity and User-Name MUST be identical. That's both reasonable, and common practice. Anything else is a nightmare.
WHERE EAP RESPONSE / IDENTITY COMES FROM

- For certificates, the EAP Identity is derived from the common name. Which is usually an email address.

- With TLS 1.2, the EAP Identity is *exactly* the certificate common name. This is fine, because the certificates are usually public. We can't do this for TLS 1.3.

- Since TLS 1.3 hides the client certificate, the EAP Identity should be anonymized, too.

- The EAP identity should be derived from the common name by using only the "@realm" portion. This derivation ensures that the authentication request is routed to the correct destination, while maintaining user privacy.
PSK IDENTITIES

- We're left with PSK Identities. For pre-provisioned identities, this is simple. We just recommend using the NAI form, and as above with certificates, using only the "@realm" portion in the EAP Identity.

- Or there may be a need for PSK Identities which do **not** match the NAI. In that case, we recommend using whatever people want for PSK Identity, **and** using "@realm" for the EAP Identity.
RESUMPTION

- The EAP application might not control the derivation of PSK identity.
- It's safest to assume that the PSK Identity is an opaque binary blob. This blob isn't UTF-8, and isn't in the NAI form, so it cannot be used for the EAP Identity.
- The only choice left when is to again recommend that the EAP Identity by "@realm".
- This allows the resumption to be routable. And decouples routing from the PSK identity. I.e. we can use a different PSK identity for every resumption. And it doesn't affect routability of the packet.
CAVEATS

- Those recommendations presume that the authentication will at some point need to be routed across a roaming consortium. If there's no roaming, then identities can be whatever format people want, and these recommendations don't matter.

- The final result then seems to be that the EAP Identity is *always* of the form "@realm". We know that works, and it isn't wrong.