E2MD Open Issues

Dean Willis, IETF 77

Is the DNS the right tech?

- Seriously debated on the list.
- Existing use cases are generally a good fit for DNS's distrribution model.
- Very close relationship to ENUM, which works well on DNS underpinnings.
- Proposed alternatives require replicating most of the DNS functions into a new protocol. Why bother?

List Conclusion:

1. DNS is the right structure.
2. We may need to offer guidance for future use cases to make sure they will fit DNS.

Issue: DNS Record Size

DNS may use UDP; leads to restrictions in DNS response packet size.

1. The E2M+type[:subtype] approach in current draft puts only one metadata value per NAPTR record, reducing size impact relative to multiple values (but may require more records).
2. Indirection with a URI can be used for larger records. Need to define "u" records for E2M:

```
$ORIGIN 3.8.0.0.6.9.2.3.6.1.4.4.e164.arpa.
@   NAPTR 10 100 "u" "E2M+cnam:https"  \
        "!^.*$!https://example.com/cnam/441632960083!" .
```

Proposed: Size is not a problem with current use cases. WG will provide guidance on size management for future registrations. Noted that EDNS0 will also help.

Issue: Privacy and Security

Some E2MD use cases propose metadata may require authenticated access. We have several possible fixes, such as:

1. Applicability statements to restrict subtype use to a private network.
2. Encrypting the sensitive data in its NAPTR.
3. Put a URI for the data into the NAPTR and use another protocol for AAA.

Proposed: For each use case, WG will evaluate sensitivity and recommend an approach. Guidelines for future E2M registrations will include guidance on handling sensitive data.

Question: Is the presence or absence of any specific record type sensitive?

Issue: How big is the auth problem?

- IF we accept that in a single DNS we will need to have differentiated access to records, then we have to provide mechanisms that support authentication and authorization for access to those records.
- What is the scale of this problem? Is it truly "Internet-scale" authentication, or is it on the order of "large web site authentication"?

Proposed: We know how to handle authentication on the "large web site" scale. Therefore, we can restrict the E2MD auth scope to fit the problem we know how to solve. E2MD will not attempt to solve the very-large scale AAA problem.

Is everything a NAPTR?

- NAPTR is queried when setting up a call.
- CNAM provides a use case for metadata not used when setting up a call but when receiving a call.
- Does this give a need for another sort of resource record used for CNAM-like things?

Proposed: WG will study this question, and if needed, choose or create an appropriate RR.