Live Summary of Mic Feedback to the Problem Statement during Discussion #1

Yes, there is a problem – where is interop needed?

Formats

- State vs. state changes
- Flexible in what to encode

Architecture

- Device (hardware or applications), relying party, attestation server
- Root of trust (not hardware root of trust); chain; how it is anchored

Transport

- Flexible transport of the "token"
- Crypto agility

Properties of the Solution

- Privacy (prevent correlation, what you send, who can see the assertion)
- Flexibility in risk model (devices can choose what to pass to who)
- Re-use protocols and work (e.g., secevents, W3C,)
- Freshness of protocol

Use Cases

- Mobile, routers/switches, PC

Open questions

- Where is the interoperability needed?
- Can a single solution be possible for all usecases?