Standardisation recap

Status update

- (Still) an *"individual"* I-D
- First published version: July 2022
- Last published version is -06 (March 2024)
- A parallel effort by Arto has been incorporated since version -05 (Arto joined in as co-author)

Goal: adoption in the TLS WG and publication by IETF with *"Proposed Standard"* status (ideally).

TLS adoption criteria

- Major extensions need formal verification (See TLS Chair's message to the mailing list)
- Interoperable implementations - mbedTLS, rustls, OpenSSL(?)
- A motivated pool of editors with the necessary TLS and IETF expertise

IAB statement on the dangers of attestation

IAB statement
CCC response
IAB response to CCC

TL;DR. There's some mistrust regarding the possibility of using attestation to restrict access to Internet public services.

IAB statement (cont.)

We need a good story for:

- Centralisation (i.e., who controls the Verifier?)

And while at it, a good analysis of:

- Privacy (especially in background-check mode)

Some of this content goes in the I-D, but we also discussed making a "living page" in the Attested TLS org, where we present a more "holistic" view of the effort with pictures, FAQs, etc.

Where does the magic happens?

Attested TLS org on GitHub
If you are in this workshop, you really SHOULD join :-)

I-D repo

IETF Slack, #attested-tls channel (ditto as per org)

Fortnightly meetings at 4 PM CET (Monday and Thursday)

Open issues

- Precise binder description
- Passport details
- Privacy & security considerations
- Editorial (clarifications, etc.)

Next steps

- Triage issues and decide what goes in the next release (hackathon)
- Address selected issues
- Publish -07 (cut-off date is 2024-07-08 by UTC 23:59)
- Ask for adoption (Vancouver? Dublin?)

Backup

Compare and contrast with RA-TLS

1. RATS "conceptual messages" (evidence and AR) as first-class credentials that can be used to authenticate the TLS handshake
2. Explicit freshness indicators
3. Intra-HS attestation

Why we think RA-TLS is not sufficient?

1. *Cute hack* that (ab)uses X.509 as a tunnelling mechanism
2. Concerns with replay opportunities / lack of explicit freshness