Running Code for ExpAt draft

Ionut Mihalcea

Many thanks to Peg Jones for kickstarting the prototyping and providing most of the implementation!

Goal

- **Have running code for draft-fossati-seat-expat!**
- Starting working towards an implementation to identify pain points
    - ... and problems in the spec
    - ... and prepare for inter-op testing when we'll have more than one implementation
- Params for this work (so far):
    - Focused on Rust
    - Adds the Exported Authenticators-based solution on top of a QUIC connection

- Library found here 🔗

State of implementation

- **It runs!**
  - Test code starts a QUIC connection over which the authenticator request and authenticator are shared.
    - Including mutual attestation.
  - Attestation evidence gathering is mocked by default, but integration with Intel TDX is available.
- Code is still WIP.
  - More work needed to add other remote attestation backends.
  - Need to integrate with a TLS library as well.

Code overview

- TLS paraphernalia
  - Fresh implementation of the TLS messages needed for RFC 9261
    - Certificate, CertificateVerify, Finished (, +Extensions)
    - With encoding and decoding functionality
- Exported Authenticators paraphernalia
  - Implementation of CertificateRequest and Authenticator
- Remote Attestation integration
  - Adds another extension type which plugs a given CMW into a Certificate message extension

Pain points

- Rust TLS ecosystem
  - rustls provides some of the crucial interfaces required
    - But does not expose code that would allow us to easily build Authenticators
    - For example, no support for custom extensions
- Remote Attestation software ecosystem
  - Dependencies also in a WIP state
    - e.g., CMW library (also implemented by us)
  - Integration with a wide variety of backends is difficult due to fragmentation
    - ratsd exists but is in active development and has no Rust client library

Bugs found in draft?

- Yes!
  - It seems we might not have implemented TLS ↔ RA binding properly.
    - Probably need to define a new keying material exporter.

Questions?