First principles (yet again)

Separating the work into two buckets:

1. Signaling
   What fields are signed, signer/verifier behavior, canonicalization.

2. Credentials
   How signers enroll, how verifiers acquire credentials, how to determine a credential’s authority for identity.
Where to look ....

Separating the work into two buckets:

1. Signaling
   - draft-ietf-stir-rfc4474bis: SIP headers, parameters, canonicalization, etc.
   - draft-ietf-stir-passport: a JSON object comprising values copied from certain header field values in the SIP request.

2. Credentials
   - draft-ietf-stir-certificates: key management
How’s it work?

Alice:
- Generates and INVITE request where the FROM header field includes her identity (address-of-record)
- Sends an INVITE over TLS to an authentication service proxy for recipients domain.

Authentication Service:
- Authenticates Alice and validates that she is authorized to assert the identity that she populated in the From header field.
- Constructs a JSON PASSporT object that mirrors particular SIP headers and fields, hashes it, signs it, and sticks it in SIP identity header.

Proxy:
- Includes pointer to certificate.

Bob’s Domain:
- Verifies the signature provided in the Identity header.

Bob’s UA:
- Can also perform validation.