Certificates Implications of Out of Band STIR
IETF 91

Reviving Out-of-Band – Why Now?

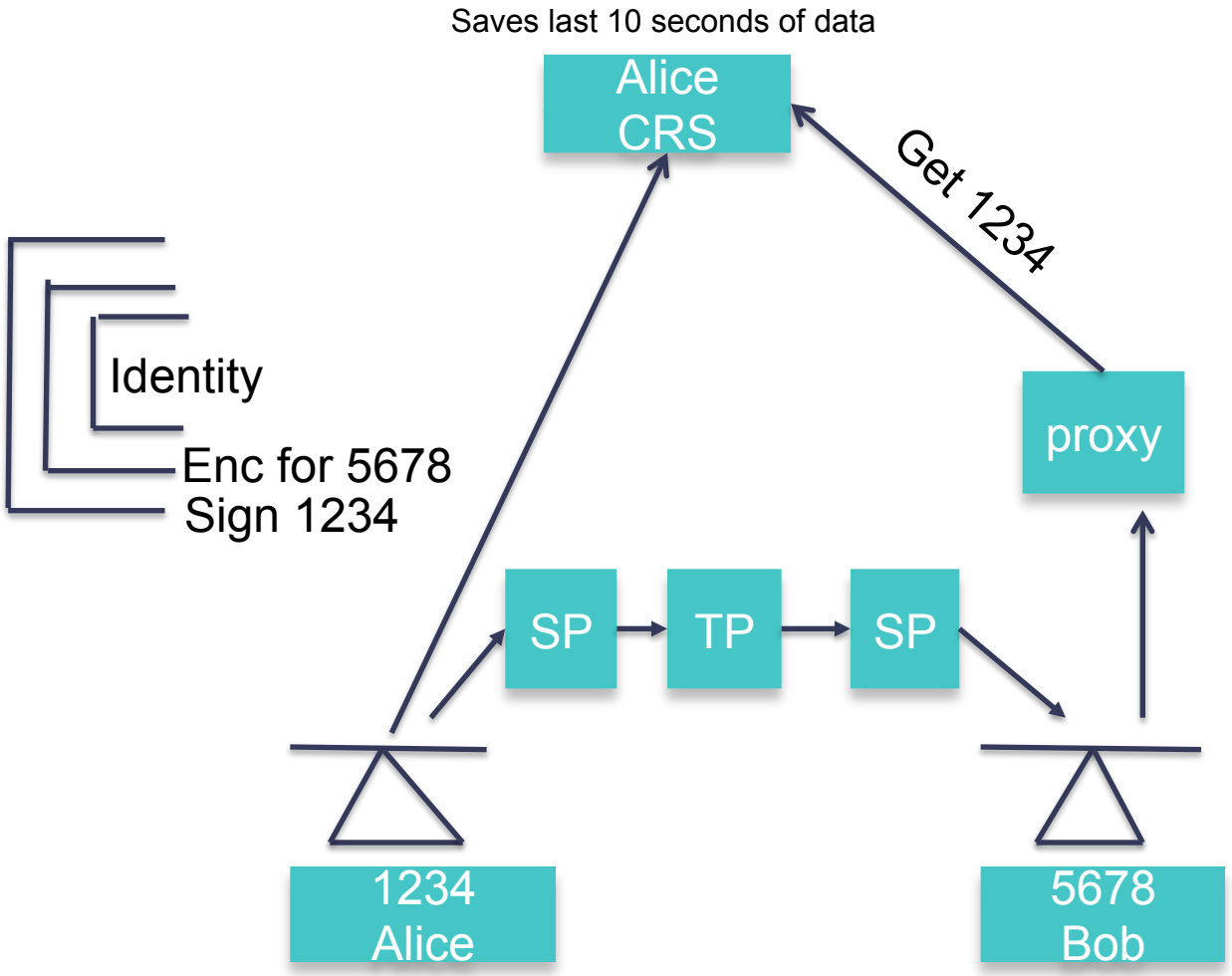
- Original charter calls for completing in-band first
- Then we split the in-band work into signaling and certs deliverables
  - Signaling work nearing completion
  - Certificates work needs to apply to both in-band and out-of-band
  - So… as we work on certs, keeping an eye on out-of-band is warranted

- First step: probably we need a baseline architecture document
  - High level decisions
  - What gets signed in the CPR?
    - RFC4474bis reduces elements signed for Identity header
      - Very similar to the list of elements signed in the CPR…
  - But today, focus on certificate questions

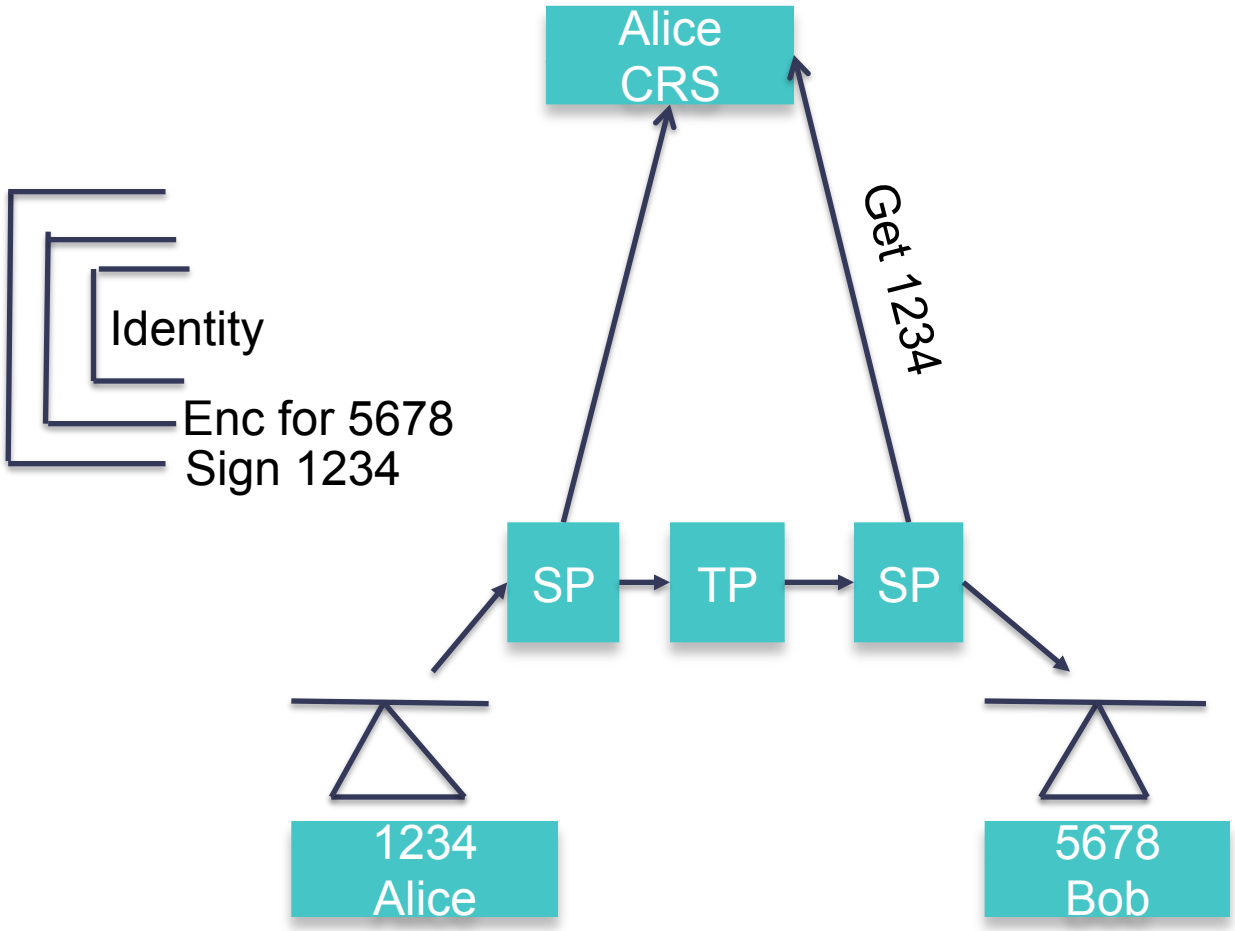
First principles

- Who interacts with the CRS?
  - Endpoints, intermediaries or both?
  - The answer is probably both
    - Endpoint support will be the easier path in some deployments
    - Intermediary support will work better in other environments
- This has large implications for cert design
  - Intermediaries could be proxies or gateways
  - Gateways may not be in the chain of number assignment
- Gateway support
    - Should PSTN gateways interface with the CRS
    - If so, what kinds of certs would they hold?
      - Is a gateway authorized to claim any number, and if so, is this a tractable approach?
      - What should the cert subject be?

Out of Band Verification (endpoint)



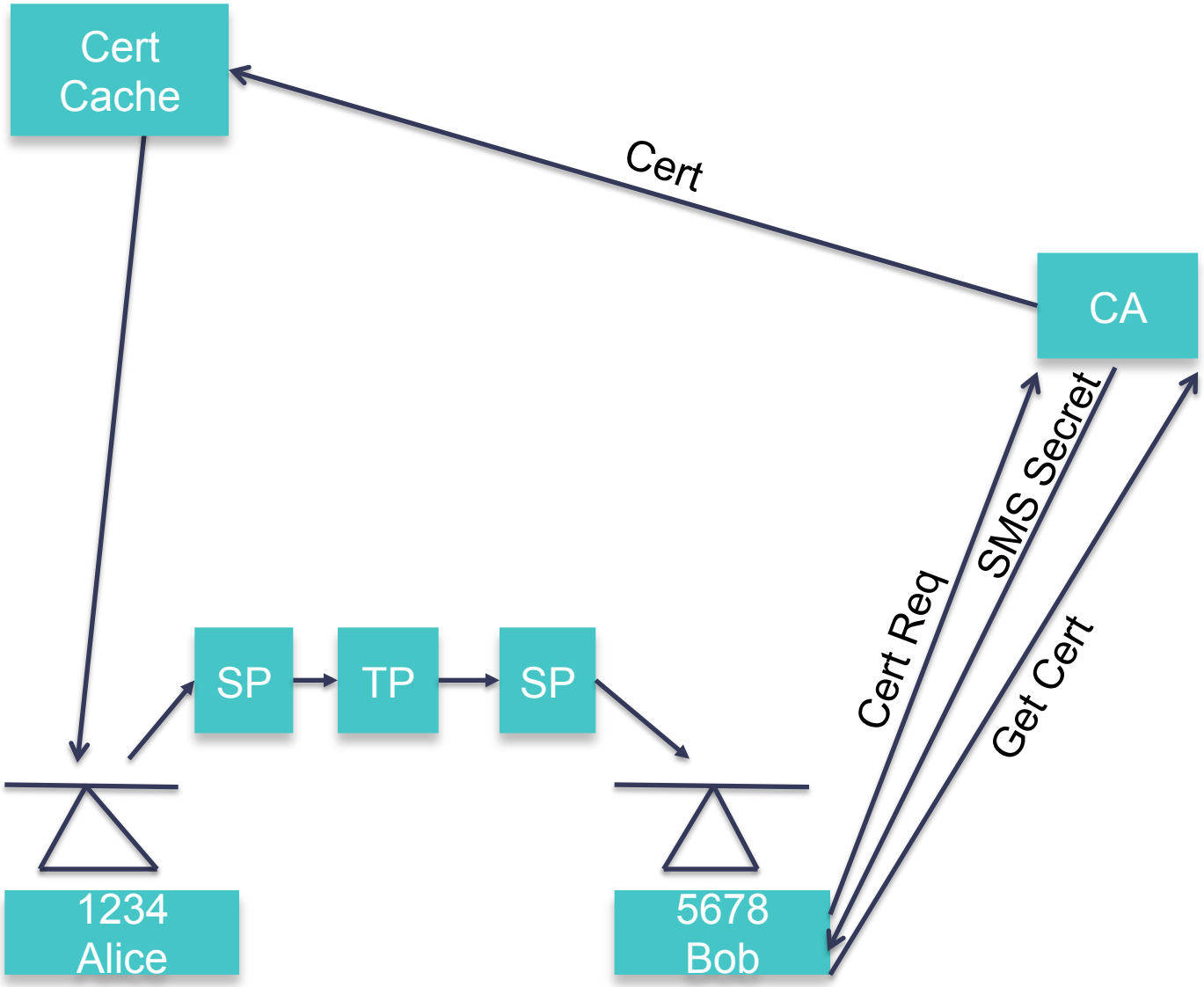
Out of Band Verification (SP)



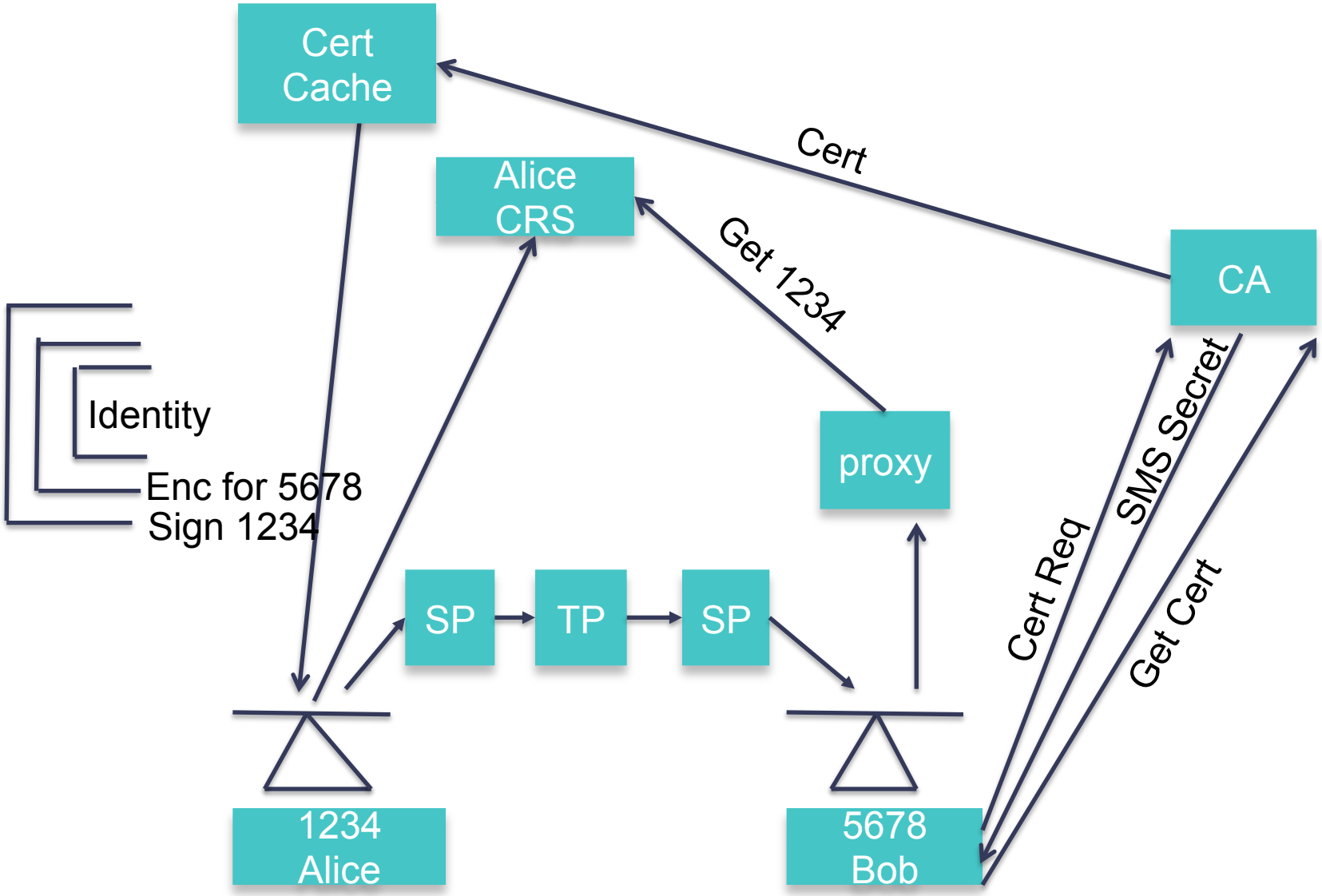
Certificates for Out-of-Band

- Three pieces of work (how separable are they?):
  - Proof-of-possession enrollment
    - How does an endpoint prove possession?
      - Classic way is via SMS with a URI, should this be codified?
    - Are there different levels of assurance for different enrollment mechanisms?
  - Proof-of-possession acquisition
    - How should endpoints get the private keying material?
      - Model one: authority creates public and private key, downloads private key to user
      - Model two: user creates public and private keys, uploads public key to authority for signing
        - How to share private key between devices?
      - Any reason not to support both?
  - Out-of-band certificate discovery
    - How does verifier discover the cert store and ask for the right cert?
    - What information is required by endpoints to identify the cert that signed a call
      - Different question that the in-band case, where Identity-Info can be assured

Cert Flow


Cert Cache
Cert
CA
SMS Secret
Cert Req
Get Cert
SP
TP
SP
1234 Alice
5678 Bob

Master


Cert Cache
Alice CRS
Cert
CA
Get 1234
Identity
Enc for 5678
Sign 1234
proxy
SMS Secret
Cert Req
Get Cert
SP
TP
SP
1234 Alice
5678 Bob