Attestation in I2NSF (and beyond)

March 2018

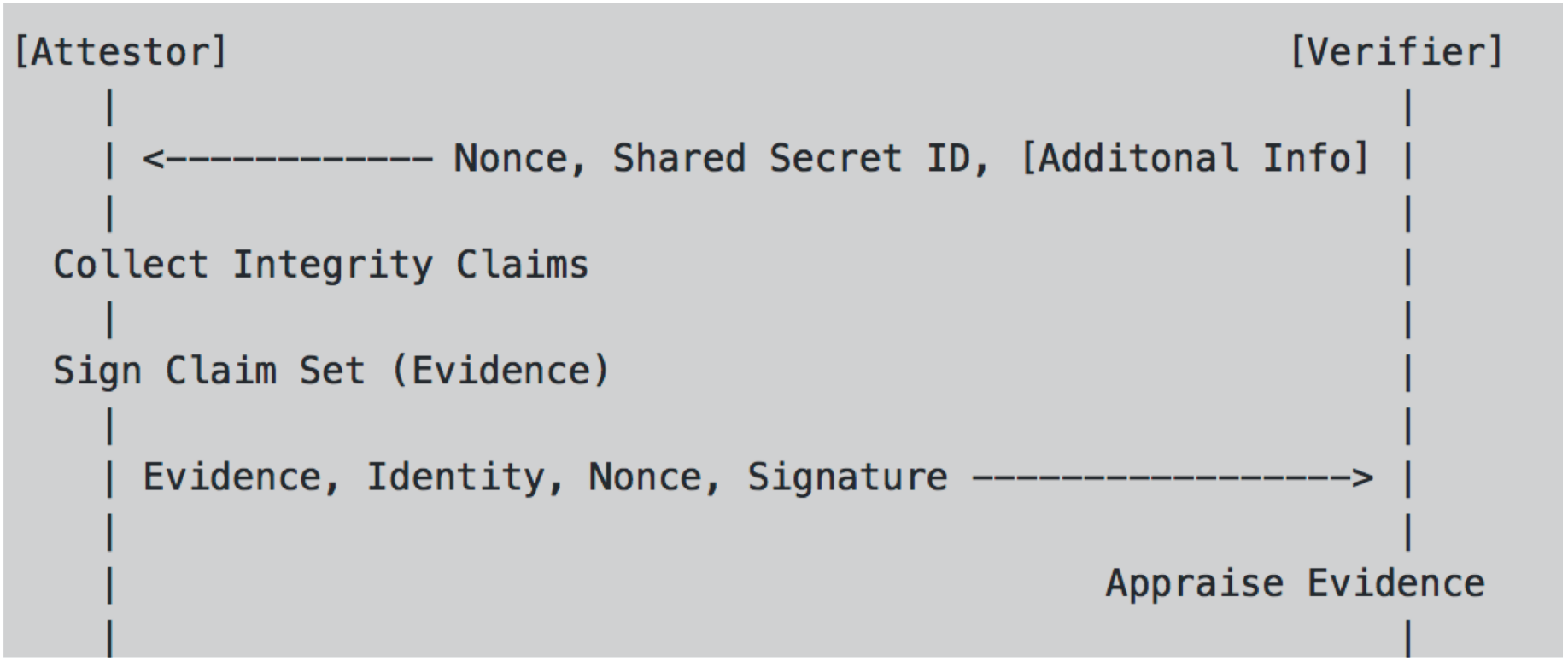
Why Remote Attestation

- Provide the consumer with evidence that their NSFs and policies are correctly enforced by the Security Controller
- Create evidence from events, suitable for auditing as a minimum, in the case of an incident.
- Allow customer to detect the alteration of the processing components, or the installation of malformed components.
- While it is true that any environment is vulnerable to malicious activity with full physical access, the application of attestation mechanisms raises the degree of physical control necessary to perform an untraceable malicious modification of the environment.
- In I2NSF, the Security Controller constitutes the natural focal point for the attestation procedures
  - Mutual authentication with a well-known point
  - Orchestration of the attestation

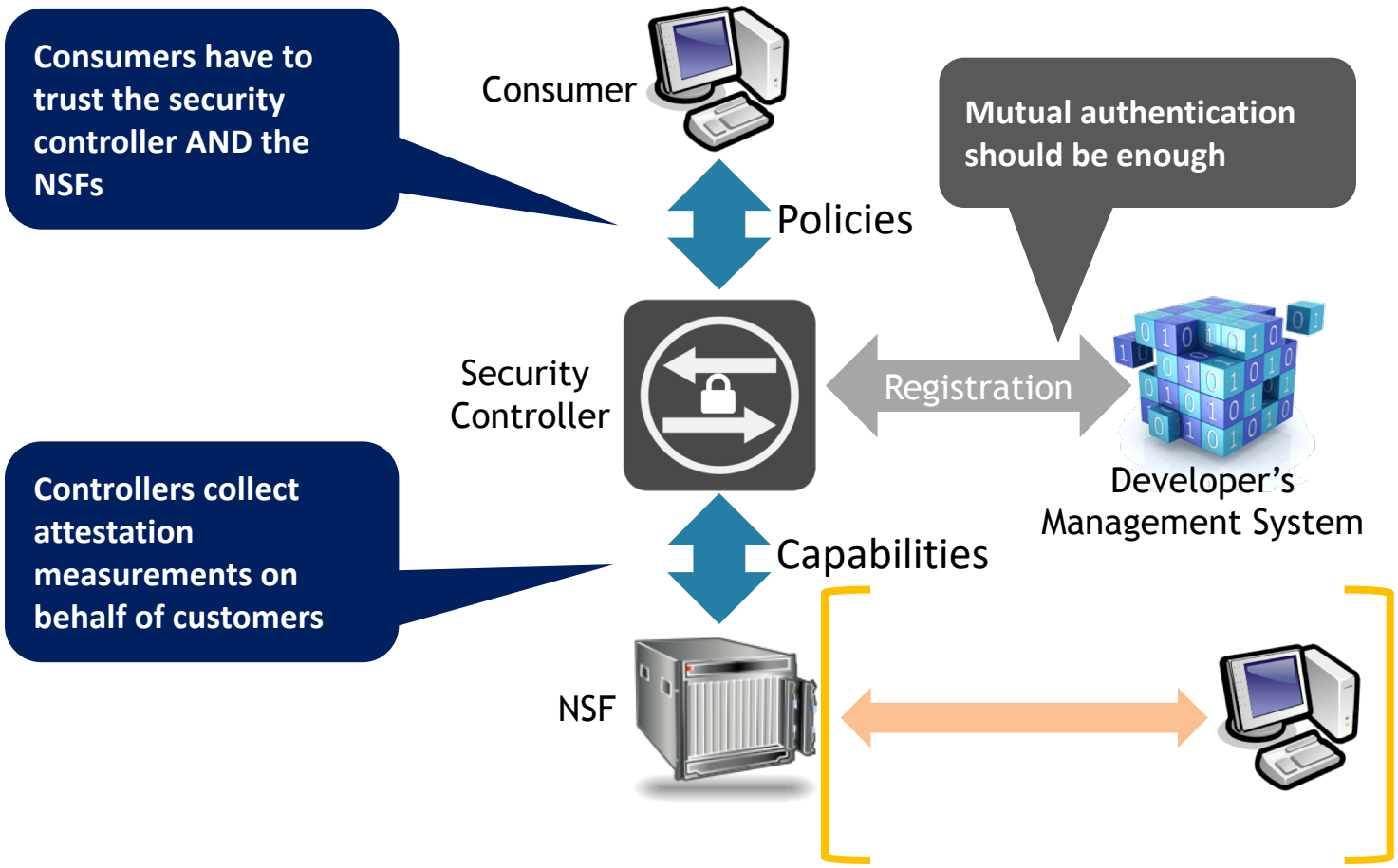
What Is Remote Attestation

- Attestation: An object integrity authentication facilitated via the creation of a claim about the properties of an attestee, such that the claim can be used as evidence.
- Conveyance: The transfer of evidence from the attestee to the verifier.
- Verification: The appraisal of evidence by evaluating it against declarative guidance.
- Remote Attestation: A procedure composed of the activities attestation, conveyance and verification.

A General Model for Remote Attestation



Attestation in I2NSF



I2NSF Remote Attestation Procedures

1. Security Controller attestation
   - The Security Controller retrieves the claims and signs them
   - The Security Controller shares the claims with the consumer
   - A TTP can be used as intermediary for the verification and supporting evidence
2. Platform attestation
   - The Security Controller makes the NSF measurements available for verification
   - Similar steps to the ones described for (2) above
   - This step can be applied periodically if the level of assurance requires it
3. Create trusted channels with the Security Controller and the relevant NSFs
   - As part of the verification process, the consumer can also check that the digest of the certificate, received during the trusted channel handshake, is present among measurements, so the channel is completely established
   - The attestation measurements allow for the use of self-signed certificates for this

And many of these procedures are applicable to other, more general, cases

Here We Stand

- Four drafts
  - draft-birkholz-attestation-terminology
  - draft-pastor-i2nsf-nsf-remote-attestation
  - draft-birkholz-i2nsf-tuda
  - draft-rein-remote-attestation-nfv-use-cases
- Plus another one in preparation
  - On a reference model for remote attestation
- Platforms for discussing and progressing general RA matters
  - https://www.ietf.org/mailman/listinfo/rats
  - https://github.com/ietf-rats
- We believe this is an essential matter for I2NSF
  - With implications beyond the WG