Remote Attestation Procedures for NSFs through the I2NSF Security Controller

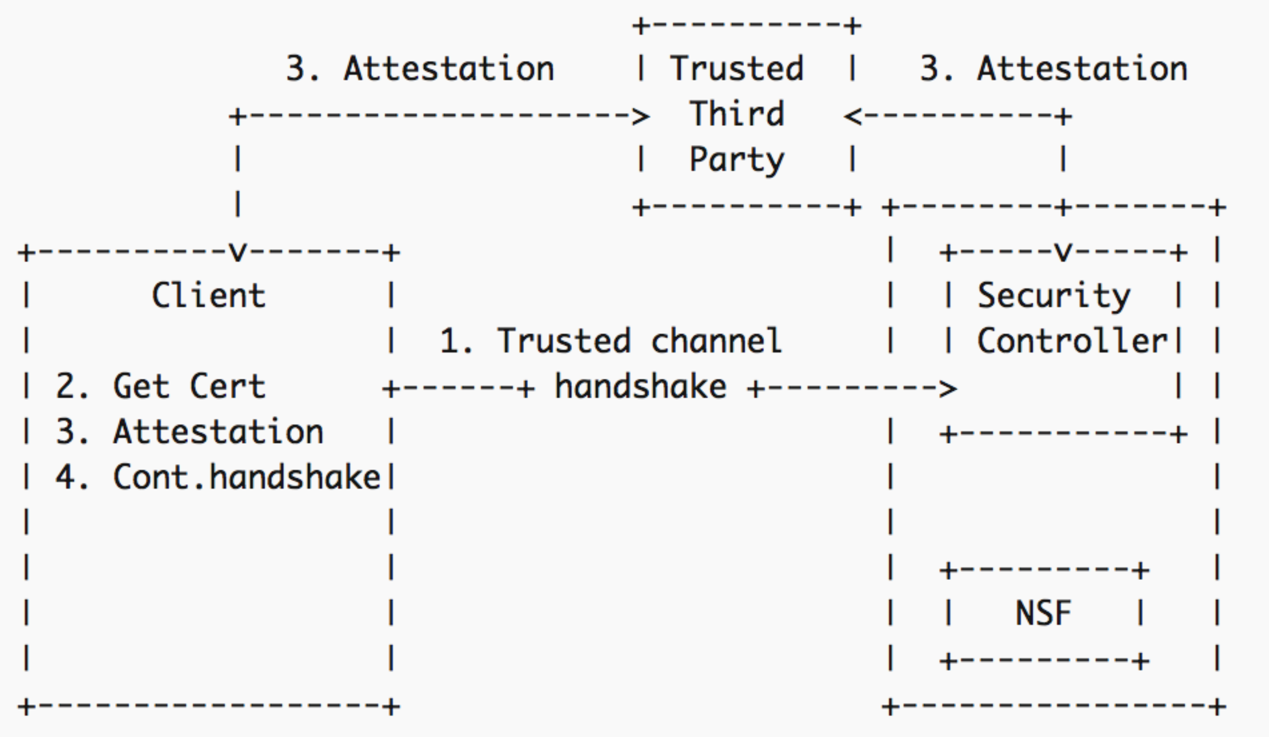
draft-pastor-i2nsf-nsf-remote-attestation(-01)

Antonio Pastor
Diego R. López
Adrian Shaw

I2NSF Meeting @ IETF98
Chicago, 27th March 2017

The (Extended) Attestation Principles

- The NSF environment runs a TPM
  - Collecting measurements of the platform, the Security Controller, and the NSFs
- Clients and the Security Controller mutually authenticate
  - Establishing a desired level of assurance



```
                                +----------+
              3. Attestation    | Trusted  |   3. Attestation
           +-------------------->  Third   <----------+
           |                    |  Party   |          |
           |                    +----------+ +--------+-------+
+----------v-------+                         |  +-----v-----+ |
|      Client      |                         |  | Security  | |
|                  |  1. Trusted channel     |  | Controller| |
| 2. Get Cert      +------+ handshake +---------->          | |
| 3. Attestation   |                         |  +-----------+ |
| 4. Cont.handshake|                         |                |
|                  |                         |                |
|                  |                         |  +----------+  |
|                  |                         |  |   NSF    |  |
|                  |                         |  +----------+  |
+------------------+                         +----------------+
```

- Trusted connection with the Security Controller
  - Or an endpoint designated by it
  - Through which all traffic to and from the NSF environment will flow
- The Security Controller makes the attestation measurements available to the client
  - Directly or through a trusted third party
    - Results from WGs such as NEA and SACM to be considered

Changes in the Latest Version

- New name, aligned with the title
  - “Virtualization Focus Has Ceased to Be”
- Updated according to the received feedback
  - Including alignment with common terminology
- Better description of the elements required to be attested
  - Grouped into the term “I2NSF platform”
  - Shall we bring it to terminology?
- Better definition of certain terms
  - Static and continuous attestation
  - Bootkit
  - Trusted channel
  - Though no need to update the terminology in this cases

The Way Forward

- Does the group believe this is a work worth continuing
- So we can start working on
  - A definition of LoAs, including the description of their requirements
    - The trusted channel and the measurements, at least
  - The usage of DAA for mutual attestation
    - At least, from the client side
  - The particular protocols to be considered
    - Look at NEA, SACM, TCG…
    - With an eye on the TEEP BoF