Remote Attestation Procedures for NSFs through the Security Controller

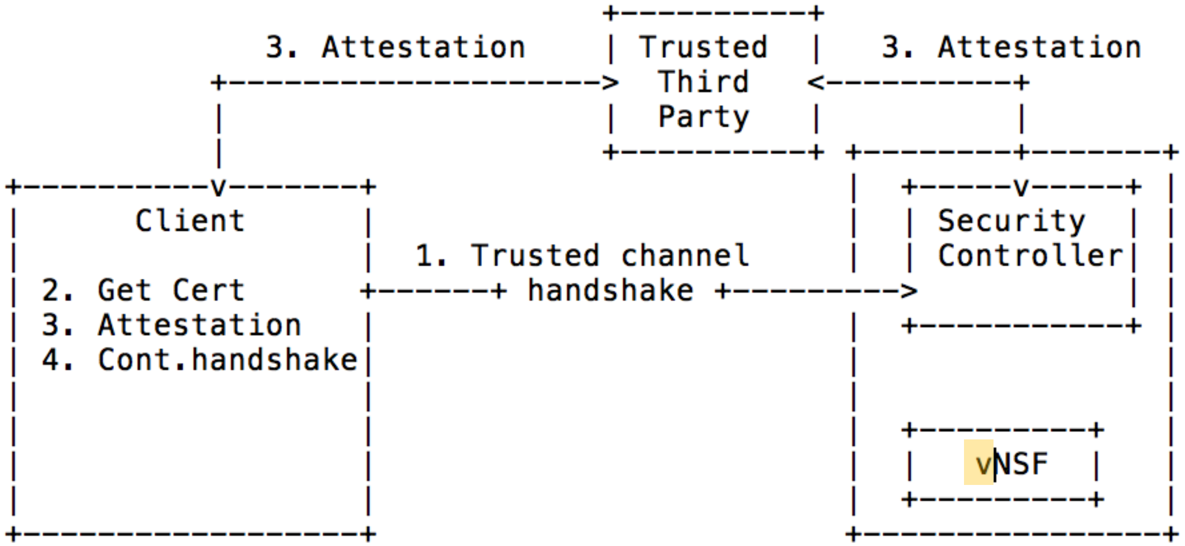
draft-pastor-i2nsf-vnsf-attestation(-03)

Antonio Pastor
Diego R. López
Adrian Shaw

I2NSF Meeting
Berlin, 21st July 2016

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|                            |                 |
|                  |                            |                 |
|                  |                            |  +----------+   |
|                  |                            |  |   vNSF   |   |
|                  |                            |  +----------+   |
+------------------+                            +-----------------+
```

- 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
  - The mechanisms for this are under evaluation
    - Results from WGs such as NEA and SACM to be considered

Changes in -03

- Align to the I2NSF terminology and framework
  - ’Client’ rather than ‘user’
  - Interfaces
  - The concept of platform/environment still open
- Sections moved to the framework document
  - Threat description
  - Requirements for a trusted client-controller interface
  - Framework referenced here
- Trusted boot description trimmed
  - Avoid too specific mentions to PCRs
- Paraphrasing Dr Strassner (and Monty Python): “Virtualization Focus Has Ceased to Be”
  - Well, almost…
- A few other text enhancements to clarify some points
  - Hopefully…
  - On the applicability of TTP, the kinds of attestation…
- The title

What To Expect of -04

- A detailed review
  - Considering consistency and alternate mechanisms
  - Thanks to John for starting this
  - We need to address the platform concept (again)
- A definition of LoAs, including the description of their requirements
  - Trusted channel
  - Remote attestation procedures
  - Somehow overdue
- A change of the name
- A request for adoption