Remote Attestation for vNSFs

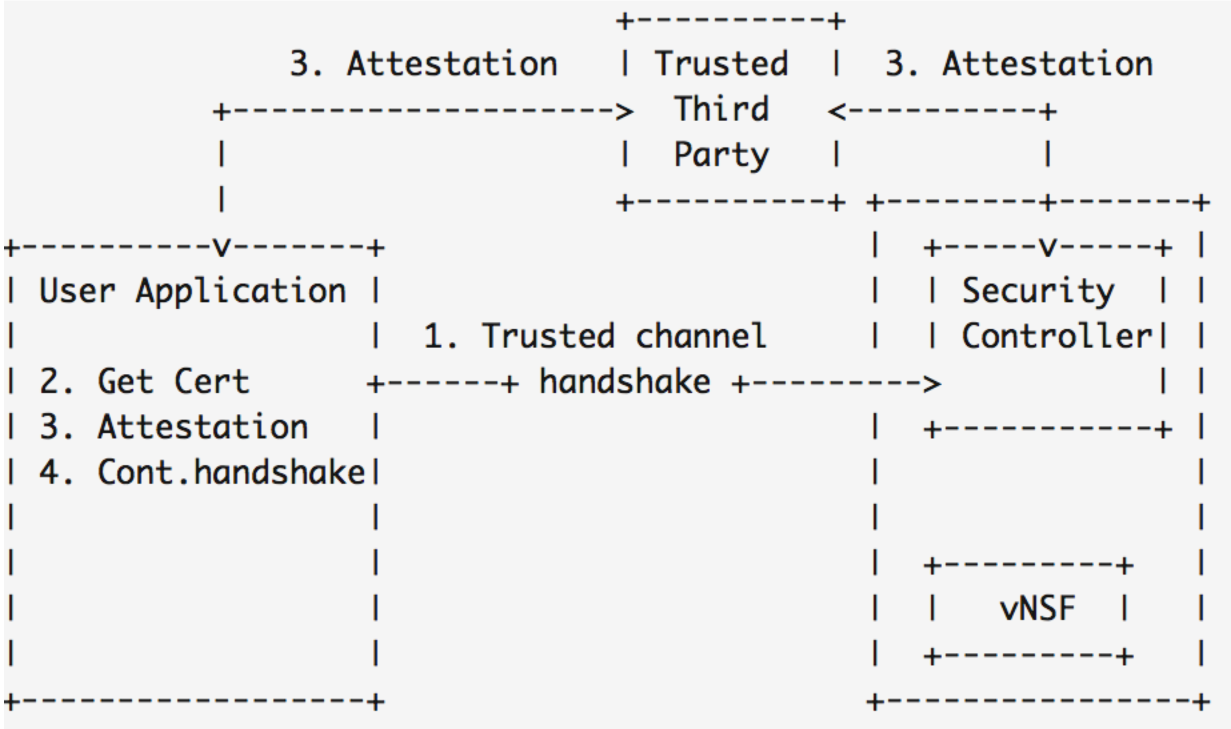
draft-pastor-i2nsf-vnsf-attestation(-02)

Antonio Pastor
Diego R. López
Adrian Shaw

I2NSF Meeting
Buenos Aires, 7h April 2016

(Restating) the Attestation Principles

- The virtualization platform runs a TPM
  - Collecting measurements of the platform, the Security Controller, and the vNSFs
- Users and the Security Controller mutually authenticate
  - Establishing a desired level of assurance



```
                                +----------+
               3. Attestation   | Trusted  |  3. Attestation
           +-------------------->  Third   <----------+
           |                    |  Party   |          |
           |                    +----------+ +--------+-------+
+----------v-------+                         |  +-----v-----+ |
| User Application |                         |  | 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 virtualized NSF environment will flow
- The Security Controller makes the attestation measurements available to the user
  - 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

(Restating) the Attestation Procedures

1. Create a trusted channel with the Security Controller
   - The establishment of the trusted channel is completed after the next step
   - The usage of a TPM and the requirements on the attestation measurements allow for the use of self-signed certificates for this
2. Security Controller attestation
   - The Security Controller retrieves the measurements and asks the TPM to sign the PCRs with an Attestation Identity Key (AIK)
   - The Security Controller shares the measurements with the user
   - As part of the verification, the application also checks that the digest of the certificate, received during the trusted channel handshake, is present among measurements, so the channel is completely established
   - A TTP can be used as intermediary for the verification
3. Platform attestation
   - The Security Controller makes the vNSFs 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

Available in -02

- Document restructuring
  - Less detailed on TCG procedures – References added
  - Document flow aligned with the principles + procedures schema
  - A discussion on how the proposed solution addresses the threats
- Description of the remote attestation procedures
  - Including an initial discussion of the different LoA properties
- Statements about the virtualization platform
  - Not a general platform any longer
  - Though most of the principles and procedures would become generally applicable

And Coming with -03

- More elaborated discussion on procedures
  - Resolving open issues and notes
- Definition of LoAs, including the description of their requirements
  - Trusted channel
  - Remote attestation procedures
- Explore the idea of considering general NSFs
  - Beyond the ‘v’ prefix…

- Provided there is interest in the community