I2NSF Remote Attestation Interface YANG Data Model

draft-yang-i2nsf-remote-attestation-interface-dm-00

Update

The following is the revise information of the original draft "trust enhanced I2NSF".

- ➢Revise the draft name to “I2NSF Remote Attestation Interface YANG Data Model”. The first reason is that it is more easy to align with RATs and the re-charter of I2NSF. The second reason is that the term of “trust enhanced” is not a specific term, which may bring in potential controversy.

- ➢Added a new paragraph about the definition of granularity of remote attestation in I2NSF. Three components in I2NSF deserve remote attestation: NSFs, basic platform, and the root of trust.

- ➢The remote attestation interface is also revised based on the granularity design. Two kinds of functions remained in the interface: RPC and notification for different component's remote attestation.

- ➢The reference value of remote attestation hasn't been defined by RATs group yet, so a temporary interface is added in the draft.

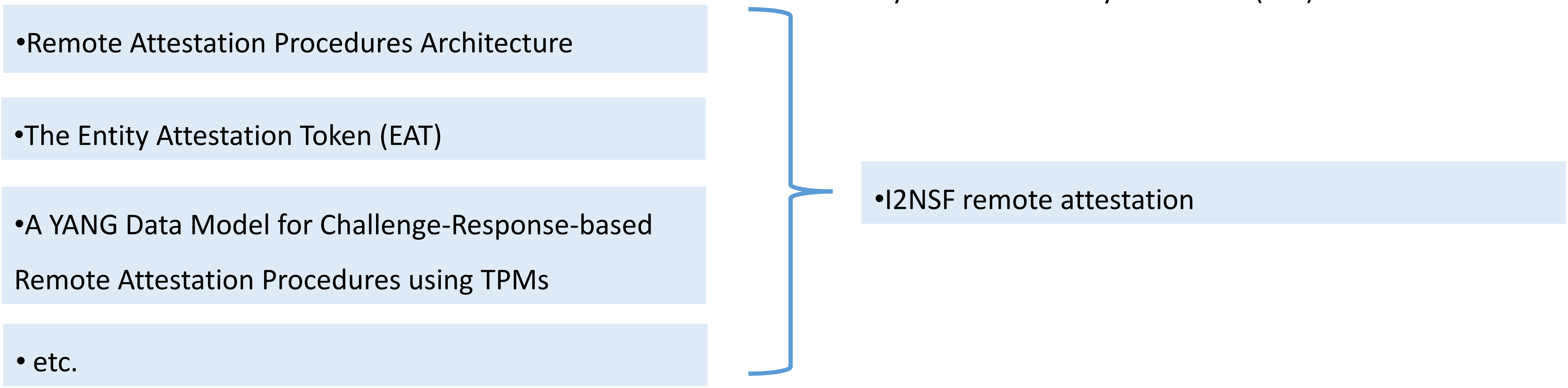
Relationship between RATs and I2NSF remote attestation

RATs:

RATs defines the basic architecture of remote attestation, different types of remote attestation evidence (e.g. based on TPM and TEE respectively), and other drafts like attestation result, etc.

I2NSF remote attestation:

I2NSF remote attestation focuses on the remote attestation of NSF in I2NSF architecture. The remote attestation target is NSF and its platform. The root of trust in I2NSF is unlimited, the Verifier and Relying Party is I2NSF Security Controller (tbd).



•Remote Attestation Procedures Architecture

•The Entity Attestation Token (EAT)

•A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs

• etc.

•I2NSF remote attestation

Necessity of I2NSF remote attestation

Security Reasons

- Inappropriate deployment of NSF.
- Potential attack by the remote platform who carries NSF.
- Security status of NSF.

Practicability Reasons

- The target and the granularity should be NSF.
- RATs architecture is inconvenient to use in I2NSF directly.
- Different device may have different root of trust, one unified remote attestation interface would be more convenient for I2NSF to implementation .

Future Extension Reasons

- Zero Trust concept may use I2NSF remote attestation to assess NSF’s trust status.
- SASE(Security Access Service Edge) may use I2NSF remote attestation to enhance edge’s security function.
- Security automation may use I2NSF remote attestation to manage NSF.
- Decentralized security intelligence sharing may use remote attestation to judge the trustworthiness of such intelligence.

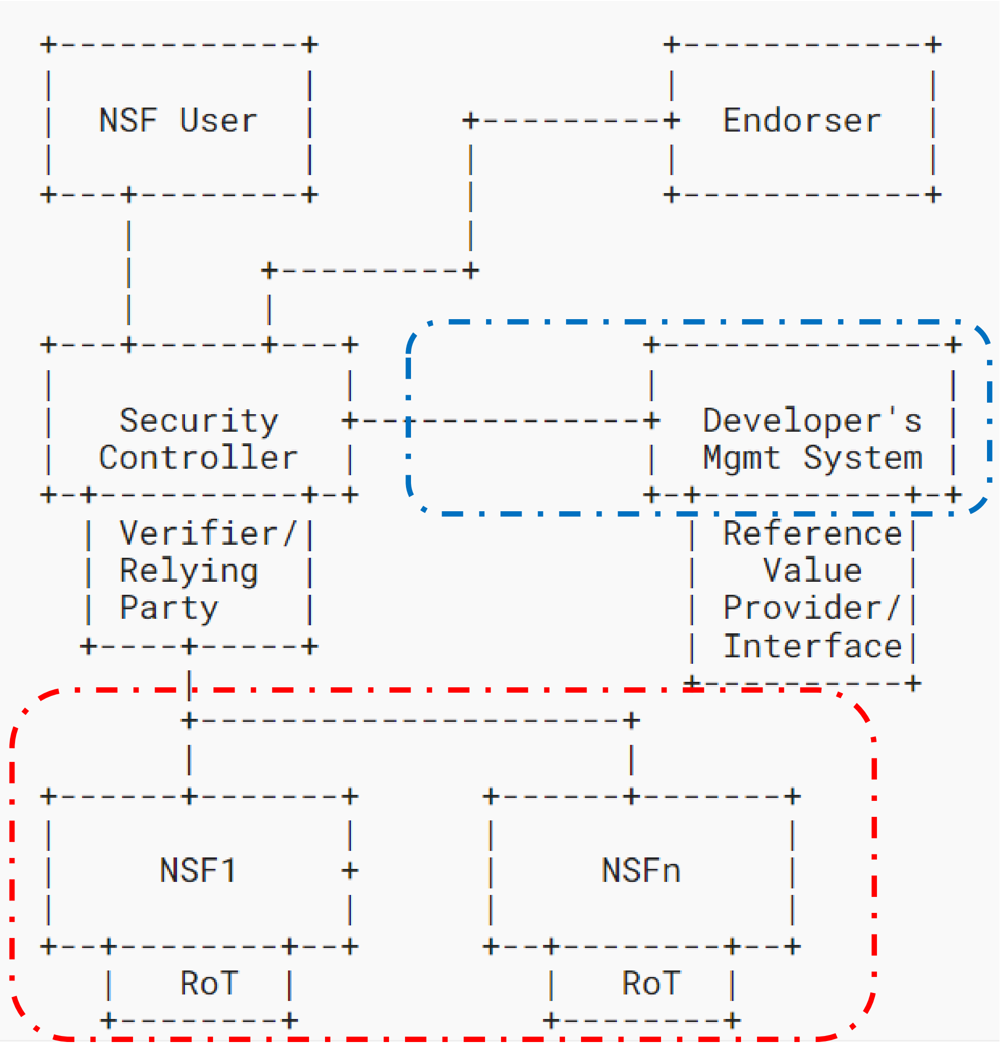
Current Interface Overview

Currently this document includes two interfaces:

➢ Remote attestation interface of NSFs and its platform. As shown in the figure, the red circle is the target that deserve remote attestation.

➢ Reference value interface from the Developer’s Mgmt system to Security Controller, as shown in the blue circle. The reference value provider may not included in Developer Mgmt System. Some other third party may also could provide reference value to Developer Mgmt System by some customized interfaces, which are not included in this draft yet.

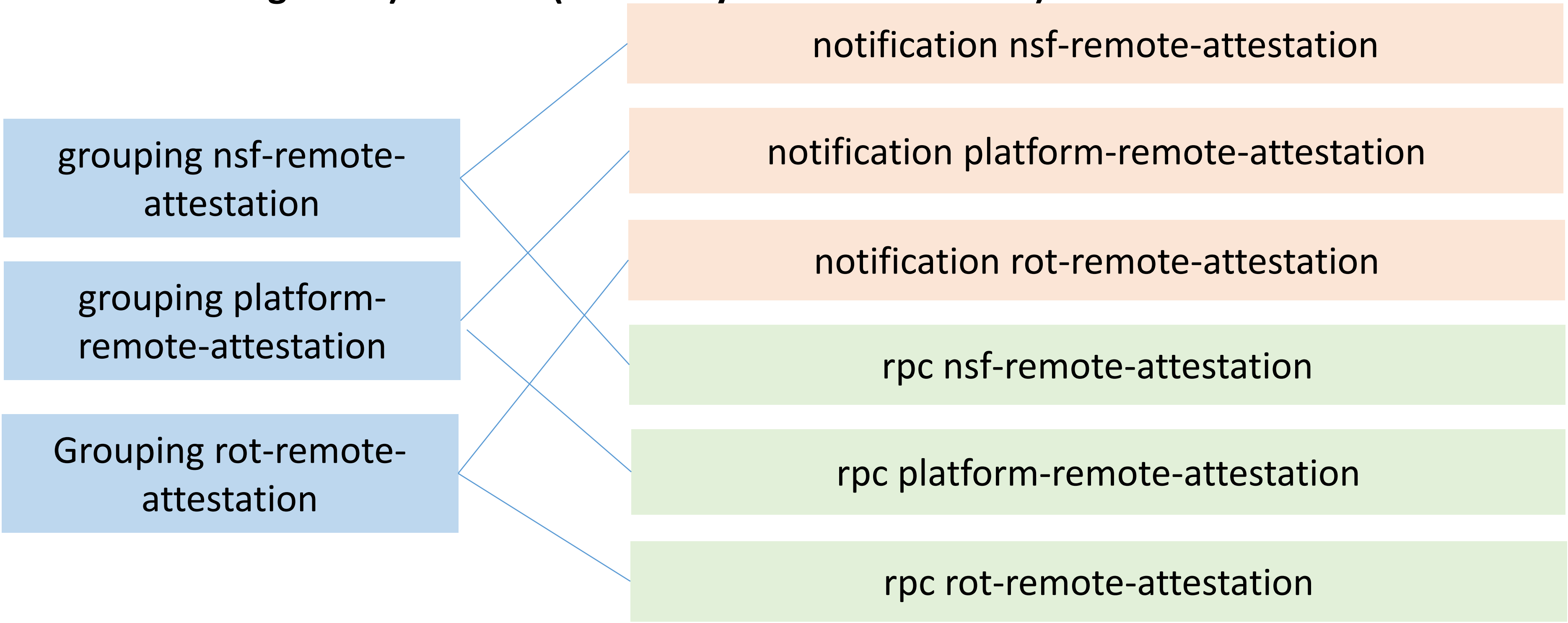
➢ The connection between Security Controller and Endorser doesn’t have to be an interface. It may be an offline method, e.g., X509.



```
+------------+                 +------------+
|            |                 |            |
|  NSF User  |       +---------+  Endorser  |
|            |       |         |            |
+---+--------+       |         +------------+
    |                |
    |      +---------+
    |      |
+---+------+---+         +--------------+
|              |         |              |
|  Security    +---------+  Developer's |
|  Controller  |         |  Mgmt System |
+-+----------+-+         +-+----------+-+
  | Verifier/|             | Reference|
  | Relying  |             |   Value  |
  | Party    |             | Provider/|
  +----+-----+             | Interface|
       |                   +----------+
       +----------------------+
       |                      |
+------+-------+       +------+-------+
|              |       |              |
|     NSF1     +       |     NSFn     |
|              |       |              |
+--+--------+--+       +--+--------+--+
   |  RoT   |             |  RoT   |
   +--------+             +--------+
```

Interface detail

- I2nsf remote attestation interface has two categories: RPC and Notification
- RPC is initiates by Security Controller, and notification is initiated by NSF when relevant events happens, e.g., the booting of platform, the loading of new nsf, the re-configuration of existing nsf.
- Reference documents mostly are Charra (A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs) and EAT (The Entity Attestation Token).



grouping nsf-remote-attestation

grouping platform-remote-attestation

Grouping rot-remote-attestation

notification nsf-remote-attestation

notification platform-remote-attestation

notification rot-remote-attestation

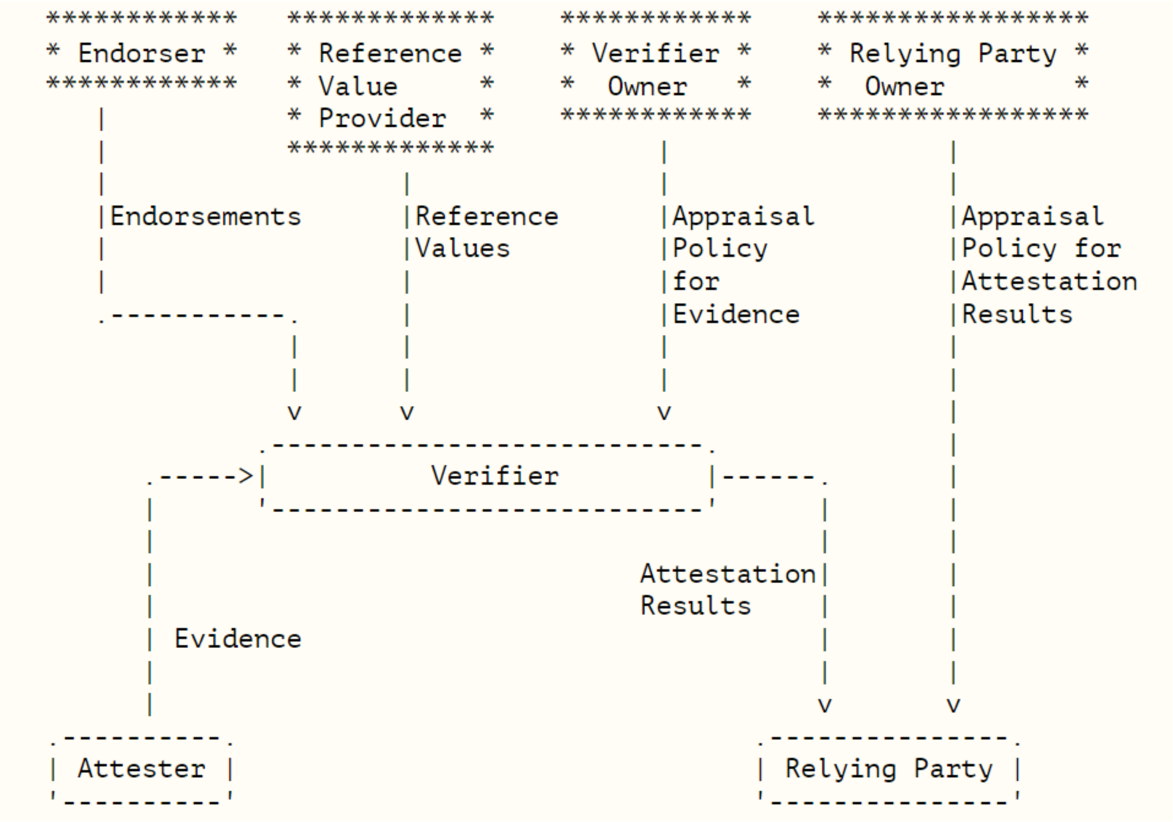
rpc nsf-remote-attestation

rpc platform-remote-attestation

rpc rot-remote-attestation

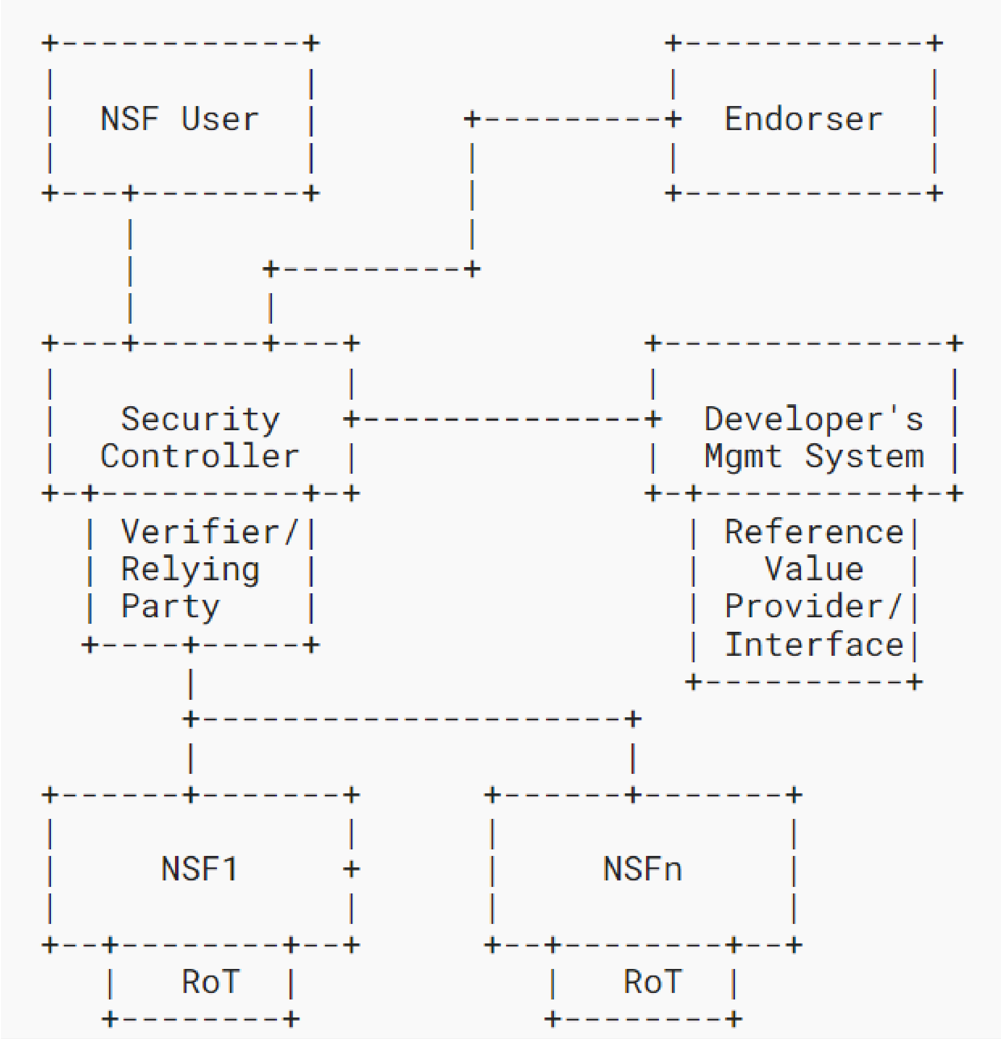
issue 1 trust model of i2nsf

Which component should be trust, which component should not be trust.



```
************   *************    ************    *****************
* Endorser *   * Reference *    * Verifier *    * Relying Party *
************   * Value     *    *  Owner   *    *  Owner        *
     |         * Provider  *    ************    *****************
     |         *************          |                 |
     |                |               |                 |
     |Endorsements    |Reference      |Appraisal        |Appraisal
     |                |Values         |Policy           |Policy for
     |                |               |for              |Attestation
     .-----------.    |               |Evidence         |Results
                 |    |               |                 |
                 |    |               |                 |
                 v    v               v                 |
               .---------------------------.            |
        .----->|          Verifier         |------.     |
        |      '---------------------------'      |     |
        |                                         |     |
        |                              Attestation|     |
        |                              Results    |     |
        | Evidence                                |     |
        |                                         |     |
        |                                         v     v
  .----------.                               .---------------.
  | Attester |                               | Relying Party |
  '----------'                               '---------------'
```

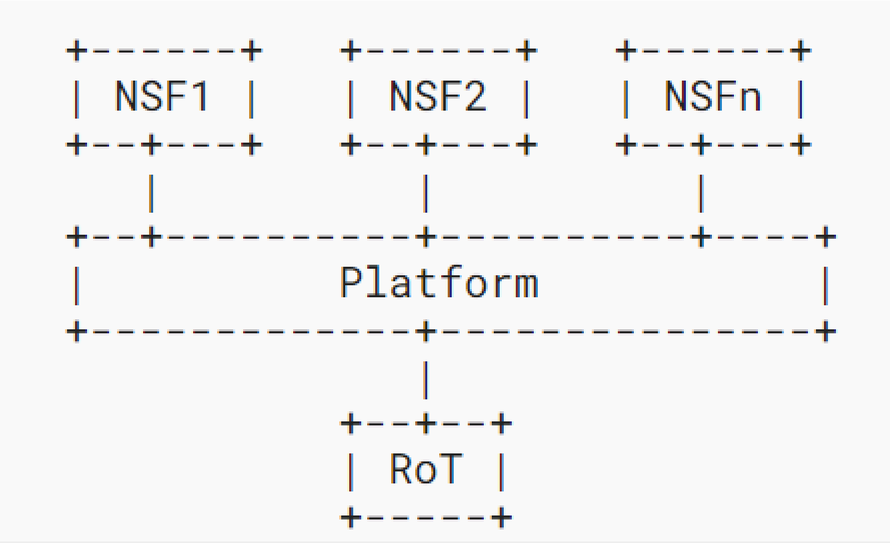
RATs architecture



```
+------------+                +------------+
|            |                |            |
| NSF User   |      +---------+ Endorser   |
|            |      |         |            |
+---+--------+      |         +------------+
    |               |
    |    +----------+
    |    |
+---+----+---+                +--------------+
|            |                |              |
| Security   +----------------+ Developer's  |
| Controller |                | Mgmt System  |
+-+--------+-+                +-+----------+-+
  |Verifier/|                   | Reference|
  |Relying  |                   |   Value  |
  |Party    |                   | Provider/|
  +----+----+                   | Interface|
       |                        +----------+
       +-----------------------+
       |                       |
+------+-------+        +------+-------+
|              |        |              |
|     NSF1     +        |     NSFn     |
|              |        |              |
+--+---------+-+        +--+---------+-+
   |   RoT   |             |   RoT   |
   +---------+             +---------+
```

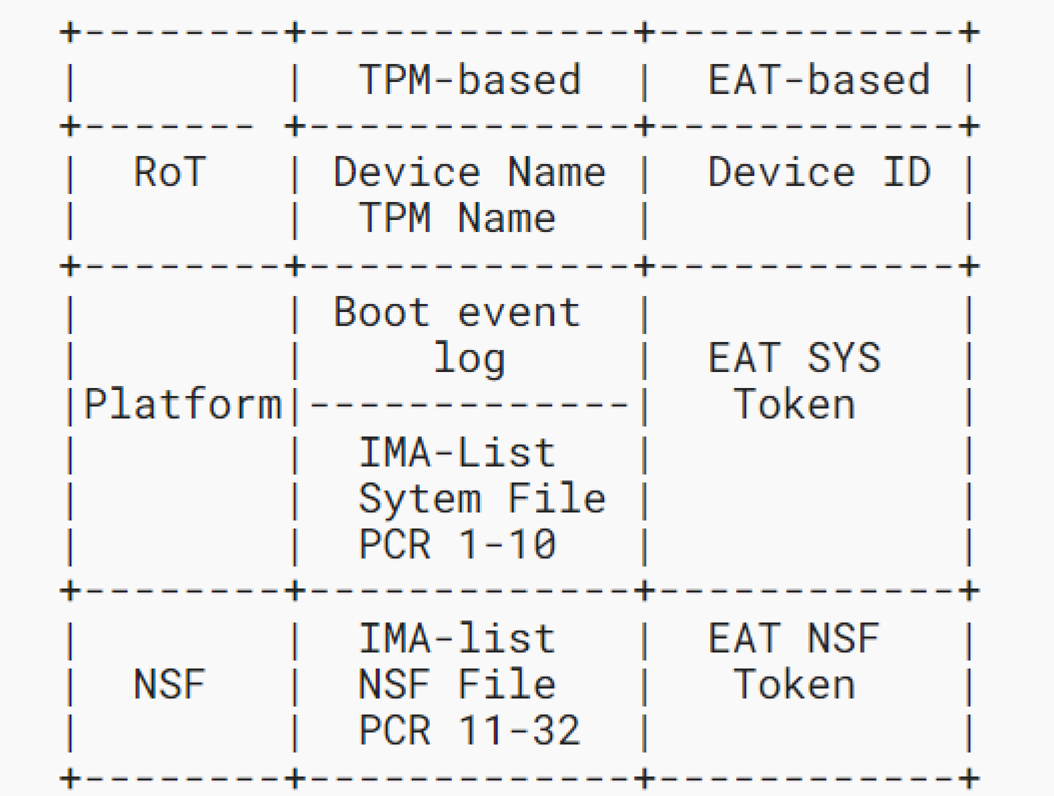
I2NSF remote attestation architecture

issue 2 granularity of remote attestation



```
+------+   +------+   +------+
| NSF1 |   | NSF2 |   | NSFn |
+--+---+   +--+---+   +--+---+
   |          |          |
+--+----------+----------+----+
|          Platform           |
+-------------+---------------+
              |
           +--+--+
           | RoT |
           +-----+
```

I2NSF remote attestation needs to define its granularity, the current granularity logic is:



	TPM-based	EAT-based
RoT	Device Name TPM Name	Device ID
Platform	Boot event log IMA-List Sytem File PCR 1-10	EAT SYS Token
NSF	IMA-list NSF File PCR 11-32	EAT NSF Token

RoT: root of trust, like TPM, TEE

Platform: the platform could be a traditional OS or a virtualization platform like Hypervisor.

NSF: If the platform doesn't support virtualization, the NSF will be an application or a process in OS. If the platform is a hypervisor, then the granularity of NSF is VM.

Thank you