Applying COSE Signatures for YANG Data Provenance

draft-lopez-opsawg-yang-provenance-02

D. López, A. Pastor (Telefónica)
A. Huang Feng (INSA-Lyon)
H. Birkholz (Fraunhofer SIT)

IETF#119, Brisbane (AU), March 2024
News on Prov·e·nance | nooz än 'prävən(ə)ns |

- Four different *enclosing methods* considered
  - As a result of the discussion within the group
  - Draft restructuring
  - Specific considerations on recursion
- Promising PoC results
  - Hoping to have a fully operational demonstrator by IETF 120
- Authors incorporated
- And a number of fixes, here and there

- To be introduced to NETMOD
Enclosing Methods – Provenance Elements

1. Add a leaf element containing a provenance signature
   • One and only one in the enclosing element
   • Anywhere

2. Include a provenance signature in NETCONF Event Notifications and YANG-Push Notifications
   • `ietf-notification-provenance` augmentation within the `ietf-notification` module

```plaintext
module: ietf-platform-manifest
   +--ro platforms
       +--ro platform* [id]
           +--ro platform-provenance? provenance-signature
           +--ro id string
           +--ro name? string
           +--ro vendor? string
           +--ro vendor-pen? uint32
           +--ro software-version? string
           +--ro software-flavor? string
           +--ro os-version? string
           +--ro os-type? string
           +--ro yang-push-streams
               |   +--ro stream* [name]
               |       +--ro name
               |       +--ro description?
               +--ro yang-library
                  + . . .

module: ietf-notification-provenance
   augment-structure /inotif:notification:
       +-- notification-provenance? iyangprov:provenance-signature

module: ietf-notification
   structure notification:
       +-- eventTime          yang:date-and-time
       +-- inotifprov:notification-provenance? iyangprov:provenance-signature
```
Enclosing Methods – Metadata

3. Include a provenance signature as metadata in YANG instance data
   • In YANG instance data files, for data at rest.

```yaml
module: ietf-yang-instance-data-provenance
augment-structure instance-data-data-set:
  +--provenance-string? provenance-signature
```

4. Include provenance signatures as YANG annotations
   • Not requiring modification of existing YANG schemas

```yaml
md:annotation provenance-string {
  type provenance-signature;
  description
  "This annotation contains a digital signature corresponding to the YANG element in which it appears.";
}
```
The Recursion Issue

- The draft only allows a provenance signature for a given enclosure
- But they can be recursive
  - Inner non-leaf elements in method 1
  - Within the notificationContent in method 2
  - Within each content-data in the instance-data-set in method 3
  - As part of the element the annotation applies to in method 4
  - Even combined at different recursion levels
- The rules for (detached) signature generation and verification are intended to support this
- Making recursive provenance validation
  - Data aggregation
  - Specific validation of relevant children
What Comes Next

- Proposal to be discussed in NETMOD
  - Comments and suggestions
  - Moving the draft there?
- Immediate work to do
  - Address sections TBD
  - Continue gathering implementation experience
- Propose adoption as soon as an operational demonstrator is available
  - Wherever…