Using Netconf Pub/Sub Model fo r RATS Interaction Procedure

https://datatracker.ietf.org/doc/draft-xia-rats-pubsub-model/

Liang Xia Huawei

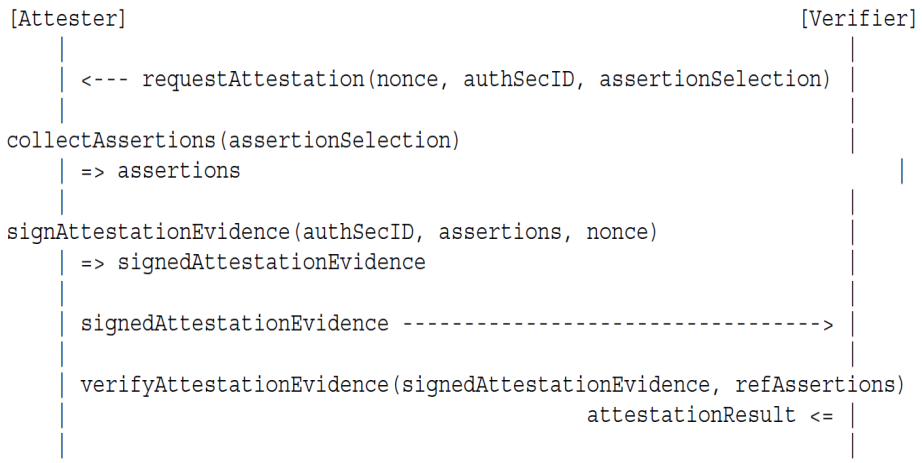
Wei Pan Huawei

IETF 106 Singapore

Interaction Mode:
Challenge & Response vs YANG pub sub & push

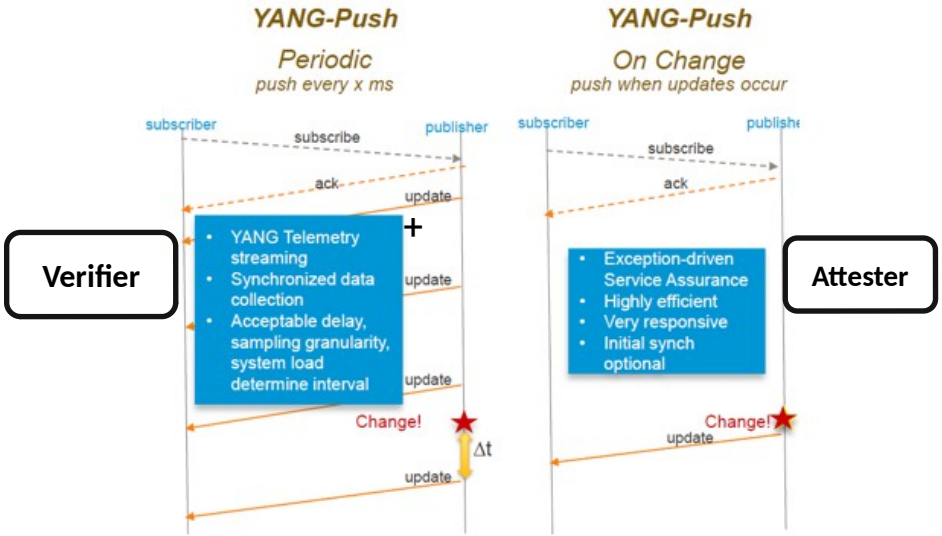
Classical mode: Challenge<->Response

draft-birkholz-rats-reference-interaction-model



Another mode: Publish<->Subscription & push

RFC 8639, RFC 8640, RFC8641



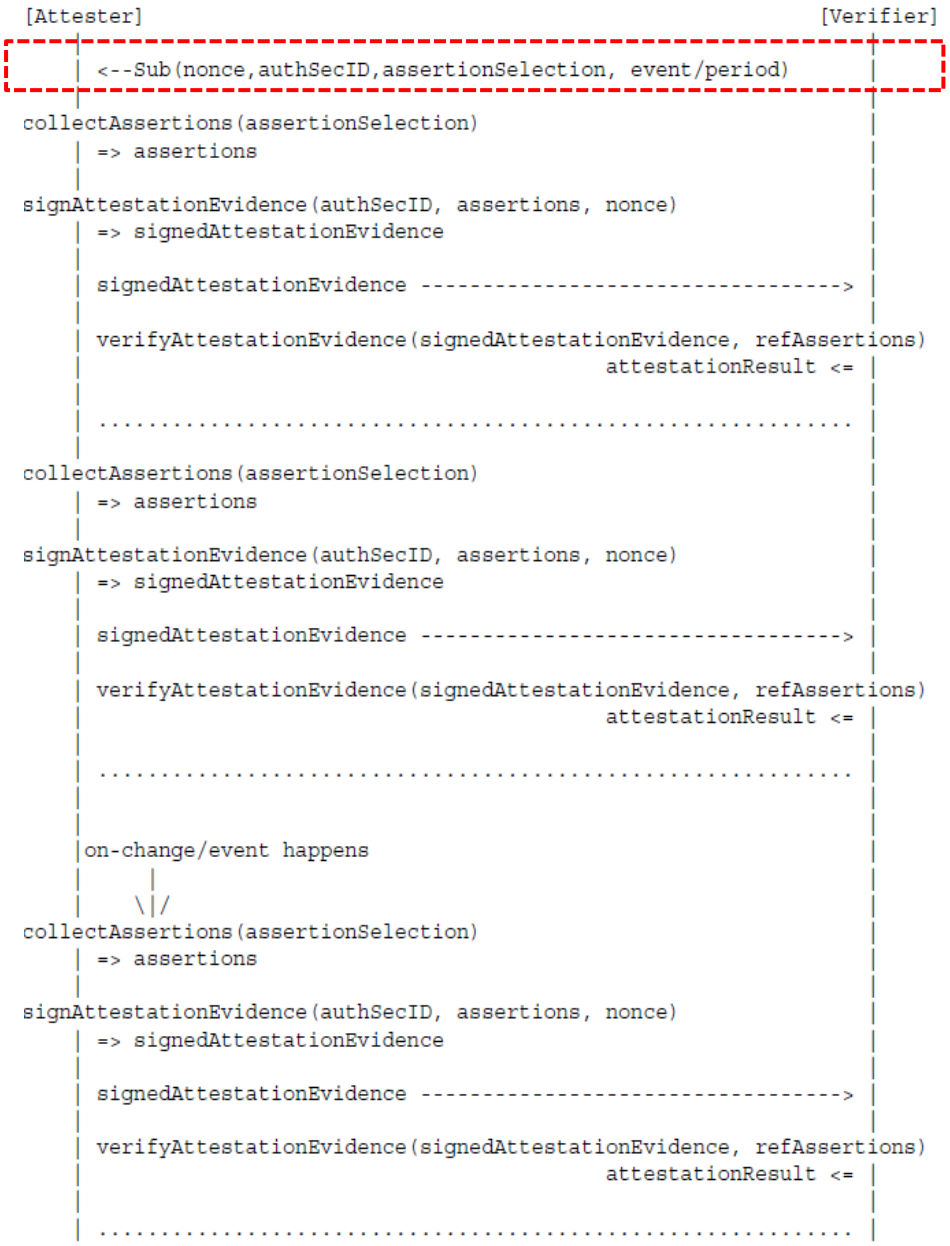
Suitable use cases: **on-demand RA**, 1:1 relationship, small or medium network…

Suitable use cases: **on-change RA**, 1:N or N:M relationship, medium or large network…

The inherited benefits of yang pub sub & push:
flexibility, efficiency, scalability, filtering capability…

RATS YANG pub sub & push model Key Points

Subscription



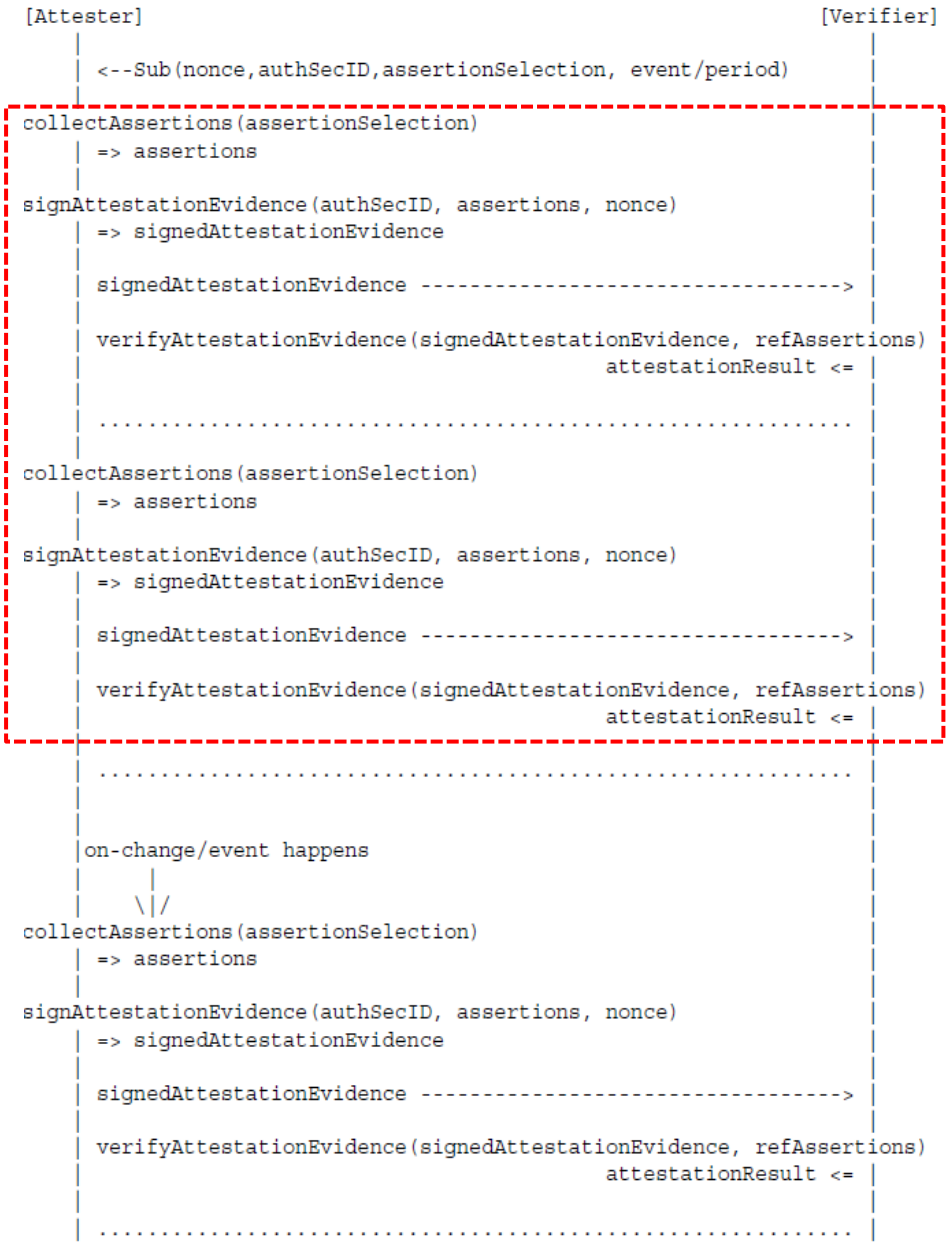
Event stream = integrity evidence

Configure subscription or Dynamic subscription are both available

Selection Filters: filter the integrity evidence based on the condition as when, where, …

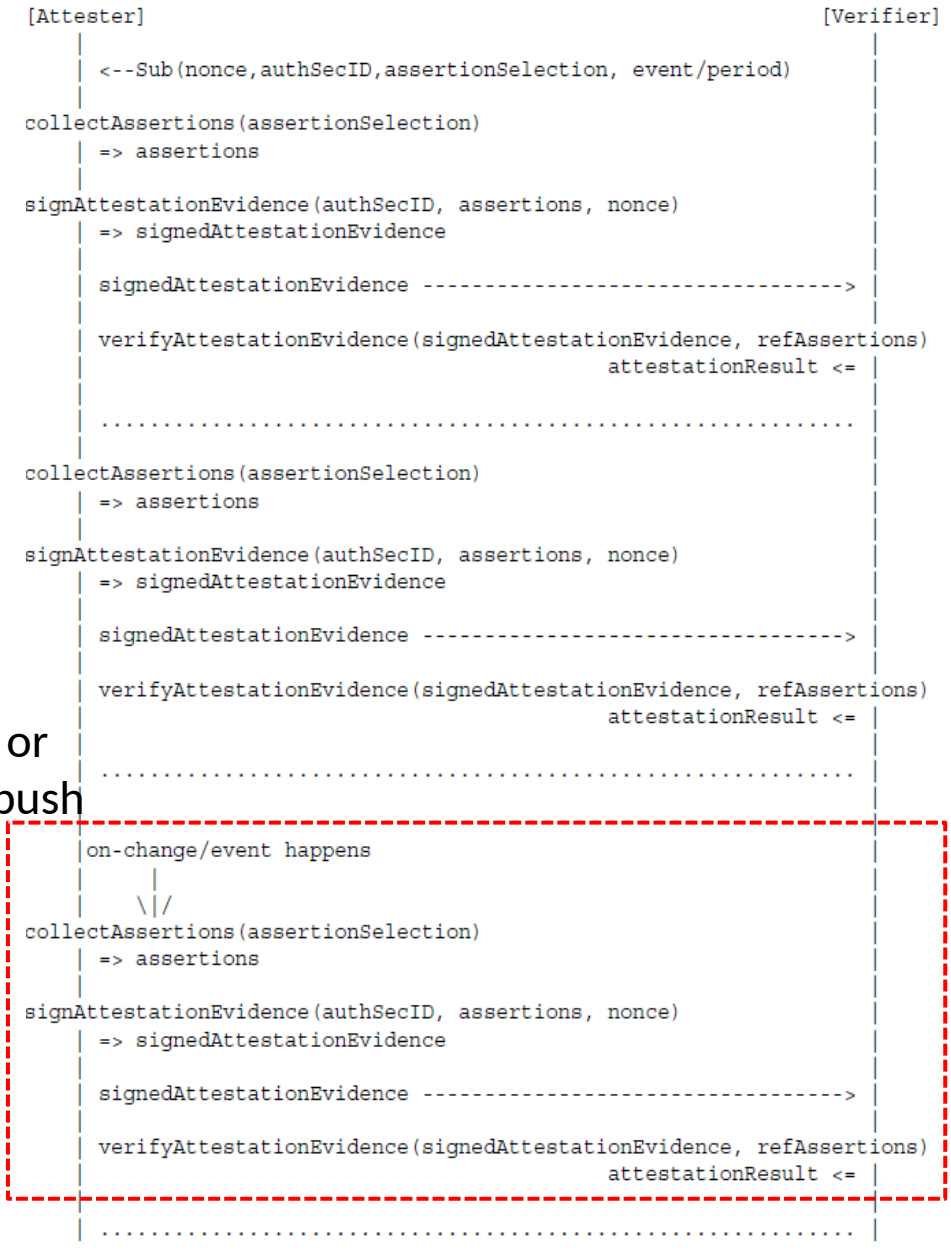
RATS YANG pub sub & push model Key Points

Periodic push



Periodic subscription: general and non-critical information collection

RATS YANG pub sub & push model Key Points



On-change push or event-triggered push

On-change subscription: monitor the critical integrity evidence when change happens

Update trigger can be pre-defined events [I-D.bryskin-netconf-automation-yang]

Remote Attestation Subscription Parameters Handling

- The RA subscription parameters are:
  - To enable the dynamic negotiation with the attester about what information the verifier nee ds and how to construct them together.
  - Originating from the RA challenge parameters.
- Generally, most of the parameters carried in the subscription message won't change during the RA procedure, like:
  - Hash signature algorithm,
  - TPM name,
  - etc.
- Nonce is for freshness validation, and a little complicated:
  - Ensure that the nonce carried in every notification message is different, and both the atteste r and the verifier know the correct value in advance.
  - Possible solutions: the timestamp or counter, the same original seed and running same RNG function at both sides, RATS TUDA mechanism [I-D.birkholz-rats-tuda].

Some Examples:
Configure subscription with on-change update trigger

```
<edit-config>
    <subscriptions
           xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
        <subscription>
            <id>100</id>
            <stream>pcr-trust-evidence</stream>
            <stream-subtree-filter>
                <xxx-vendor-device
                      xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device ">
                    <device-id>xxxxxxxxxx</device-id>
                </xxx-vendor-device>
            </stream-subtree-filter>
            <pcr-list>
                <pcr>
                    <pcr-indices>1</pcr-indices>
                    <pcr-indices>3</pcr-indices>
                    <pcr-indices>7</pcr-indices>
                    <hash-algo>
                        <tcg-hash-algo-id>TPM_ALG_SHA256</tcg-hash-algo-id>
                    </hash-algo>
                </pcr>
            </pcr-list>
            <nonce-value>0x564ac291</nonce-value>
            <TPM_ALG_ID-value>TPM_ALG_ECDSA</TPM_ALG_ID-value>
            <pub-key-id>0x784a22bf</pub-key-id>
            <tpms>
                <tpm-name>tpm1</tpm-name>
            </tpms>
            <yp:on-change>
                <yp:dampening-period>100</yp:dampening-period>
            </yp:on-change>
        </subscription>
    </subscriptions>
</edit-config>
```

Selection Filters

Subscription Parameters

Update Trigger

Some Examples:
Dynamic subscription with periodic update trigger

```
<rpc netconf:message-id="101"
       xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0">
    <establish-subscription
          xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications">
        <stream>bios-log-trust-evidence</stream>
        <stream-subtree-filter>
            <xxx-vendor-device
                  xmlns="urn:xxx:params:xml:ns:yang:xxx-vendor-device ">
                <device-id>xxxxxxxxxx</device-id>
            </xxx-vendor-device>
        </stream-subtree-filter>
        <tpms>
            <tpm-name>tpm1</tpm-name>
        </tpms>
        <last-entry-value>0xa34568baac79</last-entry-value>
        <log-type>bios</log-type>
        <pcr-list>
            <pcr>
                <pcr-indices>2</pcr-indices>
                <pcr-indices>4</pcr-indices>
                <pcr-indices>8</pcr-indices>
                <hash-algo>
                    <tcg-hash-algo-id>TPM_ALG_SHA256</tcg-hash-algo-id>
                </hash-algo>
            </pcr>
        </pcr-list>
        <yp:periodic>
            <yp:period>500</yp:period>
        </yp:periodic>
    </establish-subscription>
</rpc>
```

Selection Filters

Subscription Parameters

Period Time

Next Steps

- Get feedback from the group: are you interested? any comments?

- Keep on update: how to customize YANG pub sub & push mechanisms for the remote attestation process with its full potential?

Thank you!