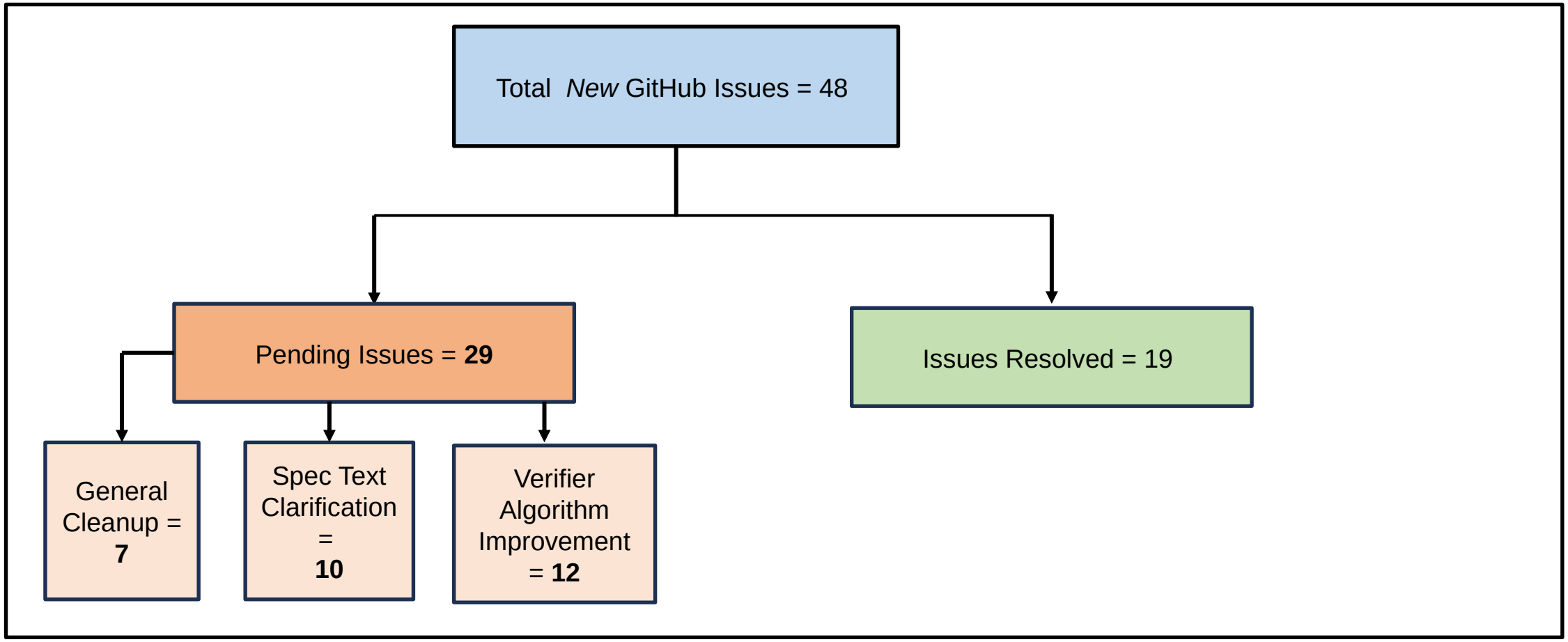
CoRIM

https://datatracker.ietf.org/doc/draft-ietf-rats-corim/06

Agenda

- Status and Progress
- General Tidy Up
- Minor additions
- Enhancements
- Verifier Phase explanation

Status and Progress (from IETF 120)



General Tidy up

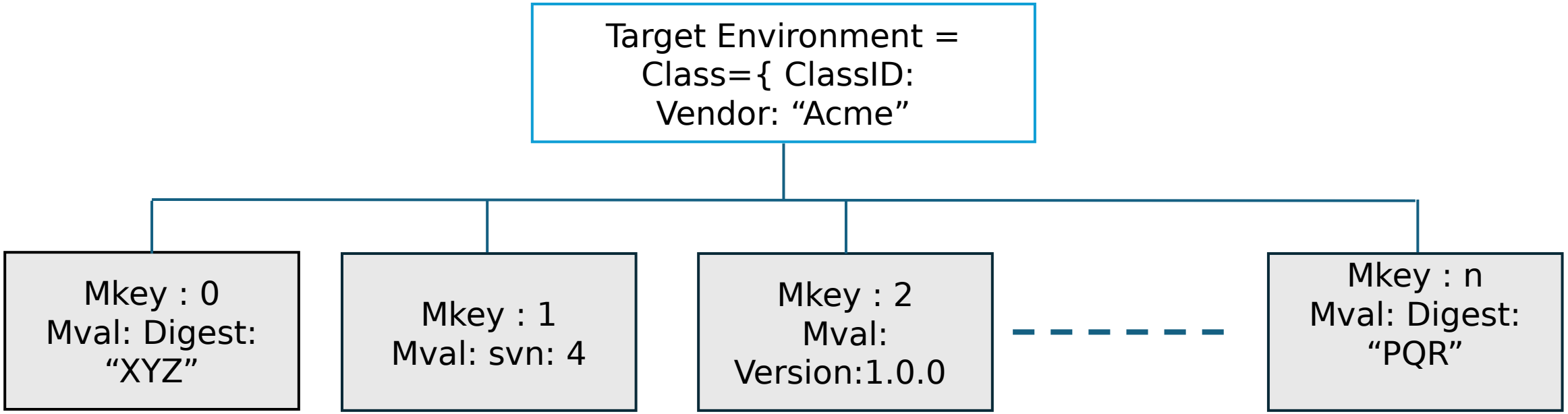
- Clarify usage of Security Version Number (SVN)
- Maintained Backward Compatibility of Code Points
- Restructured document sections (this is still WIP)
- Clarified the purpose and scope of Device Identity Triples
- Added more crisp definition of Appraisal Claims Set (ACS)
- Acknowledged contributions from Andy Draper @ Intel & Dionna Glaze @ Google
- Note: The Meeting information is now on CoRIM Repo REAMDE.md – Everyone in RATS is Welcome to attend !!

Minor additions

- Added ASN1 Der certificate type to crypto keys
- Introduced `string` type for Mkey
- Clarified Mkey extensibility
- Added Security and Privacy considerations to the base document
- Refined Corroboration text
- Added new Map Registries for CoRIM, CoMID and CoBOM maps

Major Enhancements - Multiplicity of Measurements for an Environment

1. Introduced the concept of ***Multiple Measured Elements*** for a Target Environment
2. Each Measured Element is uniquely identified by a locally scope Measurement Identity – known as **Mkey**
3. **Reference Value, Endorsed Value and Conditional Triples can now express this new addition!**



Note: *Mkey is an extensible type, with base specification defining it as oid/uuid/uint/tstr*

CDDL Impact – Base Triples

```
reference-triple-record = [
  ref-env: environment-map
        ref-claims:
    [+ measurement-map]
                        ]
```

```
endorsed-triple-record = [
 condition: environment-map
        endorsement:
    [+ measurement-map]
                          ]
```

CDDL Impact – Conditional Triples

stateful-environment-record = [env:
environment-map,
claims-list:
[+ measurement-map]]

conditional-endorsement-triple-record =
[conditions:
[+ stateful-environment-record] endorsements:
[+ endorsed-triple-record]
]

conditional-endorsement-series-triple-record = [
condition: stateful-environment-record
series: [+ conditional-series-record]]

conditional-series-record = [selection: [+
measurement-map] addition: [+
measurement-map]]

Enhancements : Clarity on Internal Representation

- Environment Claim Tuple (ECT) represents common building block structure
- Used for internal representation of Appraisal Claim Set (ACS) and various RATS Conceptual messages processed by a Verifier
- Major tidy up on ECT representation by replacing local-claim to an element-list which is of type `*element-map*`
- An element-map contains an element-id & element-claims
- Removed profiles from ECT
- Added detailed steps as to how Reference Value and Endorsed Value Triples are transformed into an ECT
- ECT Comparison sections been reworked to align with new additions

QUESTIONS