STIX & TAXII Working Call

2019-02-12

Agenda

- Presentation by Marlon from DHS on their TAXII Query / Search proposal
- Overview of where we are at with TAXII Query
- Discussion about the changes to the STIX ID
- Discussion about STIX document structure

Marlon / DHS Proposal

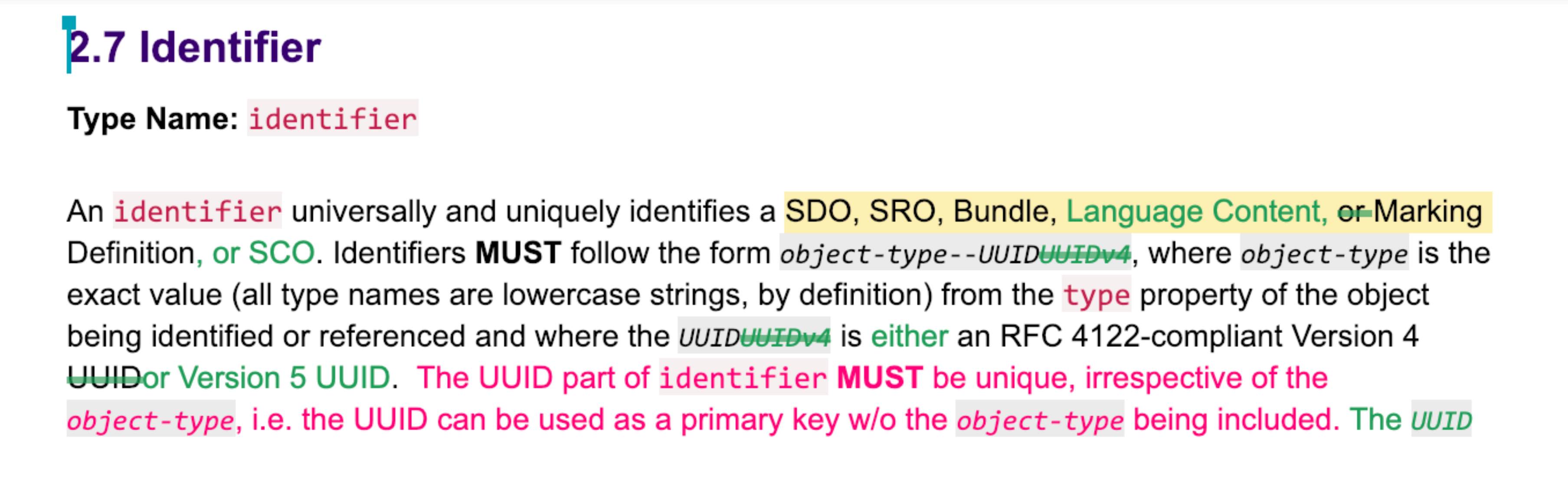
TAXII Query Overview

- Marlon just presented the DHS proposal
- I submitted a fully fleshed out proposal with text last week
- Jason will be submitting a third proposal next week
- The TC needs to decide:
  - are we going to add this for TAXII 2.1
  - if so, which proposal are we going to adopt
  - depending on the proposal, what kind of delay will that mean for TAXII 2.1

STIX ID Changes

- Sergey and others have requested that we allow UUIDv5 IDs, not just UUIDv4 IDs for STIX.
- We have worked on some text for STIX and had several people review it.
- Lets look at that text

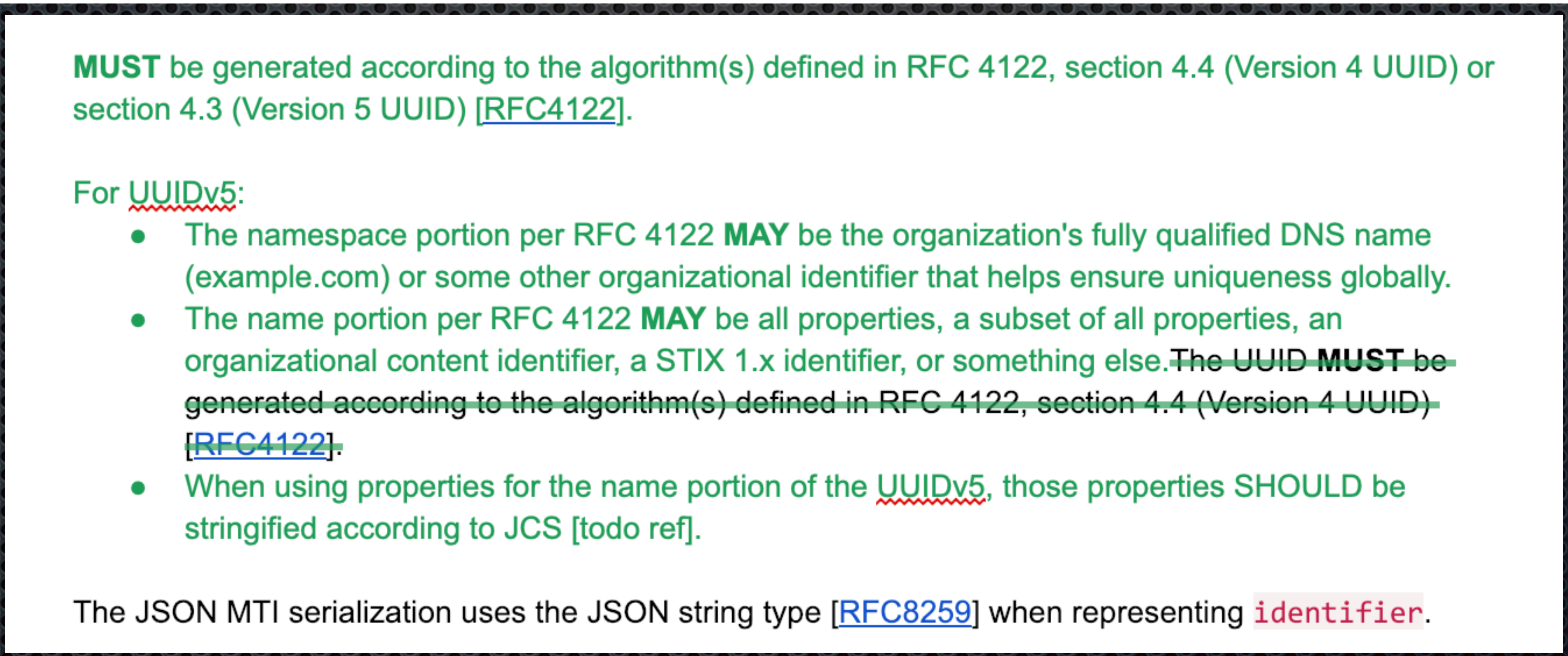
STIX ID Text



2.7 Identifier

Type Name: `identifier`

An `identifier` universally and uniquely identifies a SDO, SRO, Bundle, Language Content, ~~or~~ Marking Definition, or SCO. Identifiers **MUST** follow the form *`object-type--UUID`*~~*`UUIDv4`*~~, where *`object-type`* is the exact value (all type names are lowercase strings, by definition) from the `type` property of the object being identified or referenced and where the *`UUID`*~~*`UUIDv4`*~~ is either an RFC 4122-compliant Version 4 ~~UUID~~or Version 5 UUID. The UUID part of `identifier` **MUST** be unique, irrespective of the *`object-type`*, i.e. the UUID can be used as a primary key w/o the *`object-type`* being included. The *`UUID`*



MUST be generated according to the algorithm(s) defined in RFC 4122, section 4.4 (Version 4 UUID) or section 4.3 (Version 5 UUID) [RFC4122].

For UUIDv5:

- The namespace portion per RFC 4122 **MAY** be the organization's fully qualified DNS name (example.com) or some other organizational identifier that helps ensure uniqueness globally.
- The name portion per RFC 4122 **MAY** be all properties, a subset of all properties, an organizational content identifier, a STIX 1.x identifier, or something else.~~The UUID **MUST** be generated according to the algorithm(s) defined in RFC 4122, section 4.4 (Version 4 UUID) [RFC4122].~~
- When using properties for the name portion of the UUIDv5, those properties SHOULD be stringified according to JCS [todo ref].

The JSON MTI serialization uses the JSON string type [RFC8259] when representing `identifier`.

STIX Document Structure

- STIX and CybOX were developed semi-independently and were purposefully kept as separate documents
- We merged STIX and CybOX (now Cyber Observables) but kept the documents pretty separate for STIX 2.0
- STIX Part 1 and Part 2 used to be a single document just like Part 3 and Part 4 used to be a single document, however Google Docs has a hard time dealing with large documents

STIX Document Structure

- Right now we have 5 parts for STIX.
- It is a bit challenging for people to find to find where things are, unless they are really familiar with the content.
- We have a lot of unnecessary redundancy in the documents due to OASIS templates requirements, this makes keeping everything in sync a bit harder to do

STIX Document Structure

- Cyber Observables are not becoming top-level objects likes STIX Domain Objects or STIX Relationship Objects, but they are moving closer to the STIX world
- There is a lot more overlap now, given the proposed changes to Cyber Observables
- I personally believe this is going to make things even more confusing for consumers of this specification

Proposal

- I would like to separate the concepts of:
  - How many documents do we need to efficiently do editorial work and get feedback form the TC from
  - How should the final documents be packaged and delivered as a final work product
- For the final release, NOT the daily working editorial / TC feedback documents, I believe we should collapse our 5 documents down to 4

Proposal

- Document 1: STIX Core Concepts
    - This will include all of the core concepts that are in Part 1 today and some of the content that is in Part 3 today. So all “core concepts” will be in a single place

Proposal

- Document 2: STIX Core Objects
  - This will include the common properties for core objects
  - SDOs, SROs, Bundle, Marking Definition, and Language objects.
  - Vocabs
- Basically everything a developer would need to implement STIX in code, once they understood the core concepts.

Proposal

- Document 3: Cyber Observable Objects
  - This will include the common properties for Cyber Observable objects and the Cyber Observable Container for legacy support for Observed Data
  - All of the Cyber Observable Objects themselves
  - All of vocabs that are specific to Cyber Observables
- Basically everything a developer would need to implement Cyber Observables in code, once they understood the core concepts.