

Scope

Describe traces from digital or physical resources to support cyber-investigations

RDF-oriented ontology:

- release versioning
- trace descriptions
 - ontology release version (mandatory)
 - metadata using duck-typing
 - data (included / referenced)
- provenance (chains of evidence and custody)
- marking / classification
- relationships between traces
- natural language glossary
- licensing

Tools:

- application programming interfaces
- validators
- translators
- proof of concept implementations
- support tool-specific mappings
- licensing

Issues

General:

- no end-users (investigators/prosecutors) involved
- not all major tool providers involved
- No flyer/one-pager available

Ontology:

- release versioning not defined / available
- no mandatory version in CASE expressions
- no best practices, e.g.
 - referencing / including data
 - unsupported property bundles
- conflicting semantics, e.g.
 - Contact vs. PhoneAccount

Tools:

- no support for Java, C#, and JSON-LD languages
- no validator

Events:

- mapping and implementation workshop
- vendor customer feedback (survey as well)
- ontology conference/workshop

Global meetings:

- no (issue-based) agenda for meetings (add to governance model)
- update on website

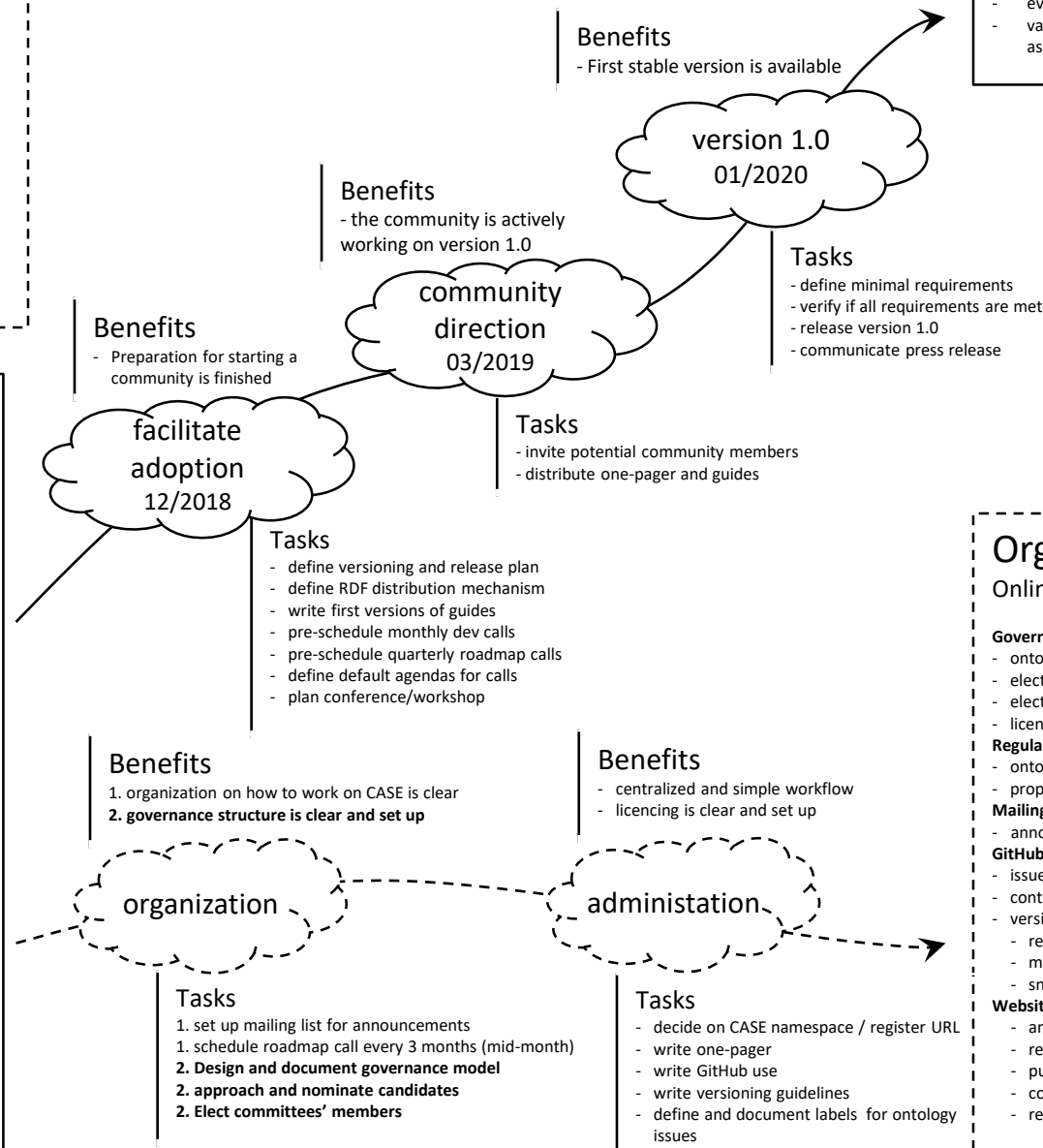
Add to Governance Model:

- declare mailing lists (announcements)
- declare establishing dates for roadmap review
- declare create a nonprofit or organization to hold URL namespace
- declare governance/licensing documentation
- declare periodic review of major milestones (assigned to Github)
- declare global meeting agenda

CASE roadmap

Cyber-investigation Analysis Standard Expression

DRAFT - version 2018-09-19



Goals

All major tools provide a mechanism for importing and exporting CASE expressions.

CASE is actively used to:

- support investigations
- evidence exchange
- validate tools (based on ground truth available as CASE expression)

Organization

Online community

Governance structure

- ontology & governance committees
- election protocol
- election protocol
- licensing

Regular (virtual) community meetings:

- ontology directions
- proposal/change decisions

Mailing list:

- announcements (same as website)

GitHub:

- issue tracking, bugs, proposals
- continue updating guides
- versioning
 - releases
 - milestones
 - snapshots (work in progress)

Website (Community Portal):

- announcements tab (same as mailing list)
- recorded meetings tab (hosting platform?)
- publications tab
- contact tab (mailing list subscriptions)
- release tab (RDF ontology releases)