TRUST Over IP FOUNDATION

THE LINUX FOUNDATION

The ToIP Interoperability Certification Framework

A Proposal from Avast

Drummond Reed
Allan Thomson
Charlie Walton

Wednesday, 26 October 2022
12-13:3O PT / 20:00-21:30 UTC

Proposed Strategic Objective

The JDF charter of the ToIP Foundation includes the following scope statement (emphasis added):

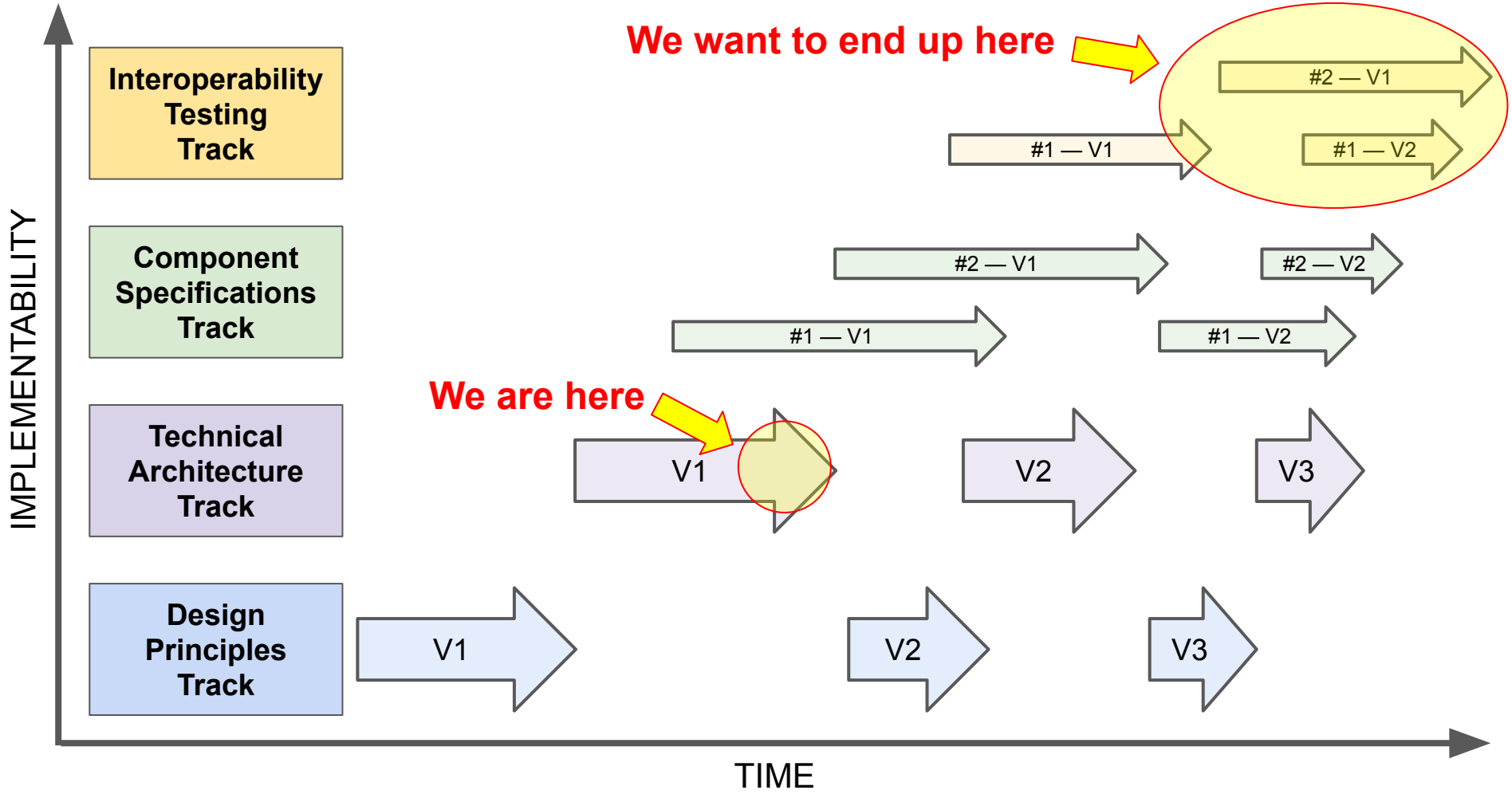
The purpose of the Trust over IP Foundation (alternatively, "ToIP Foundation") is to define and support a complete architecture and interoperability certification framework for Internet-scale digital trust that combines both cryptographic trust at the machine layer and human trust at the business, legal, and social layers as defined in Hyperledger Aries RFC 0289 (or its successor as identified in the RFC document itself).

Proposed Strategic Objective

The process of producing the first version of our **ToIP Technology Architecture Specification** (TAS) resulted in excellent discussions about our the overall roadmap and the specific development tracks we are following to fully realize the ToIP stack.

It resulted in the recommendation that we should produce a companion document called **Evolution of the ToIP Stack** that lays out this roadmap and explains the purpose and progress of each development track.

The following diagram is the centerpiece of that document (and is included in the introductory sections of the TAS).


We want to end up here
#2 — V1
#1 — V1
#1 — V2
Interoperability Testing Track
Component Specifications Track
#2 — V1
#2 — V2
#1 — V1
#1 — V2
We are here
Technical Architecture Track
V1
V2
V3
Design Principles Track
V1
V2
V3
IMPLEMENTABILITY
TIME

Proposed Strategic Objective

Avast would like to propose that the Steering Committee make it an **explicit strategic objective** of the Foundation to establish an interoperability certification framework **within two years** of publishing our V1 **ToIP Technology Architecture Specification**.

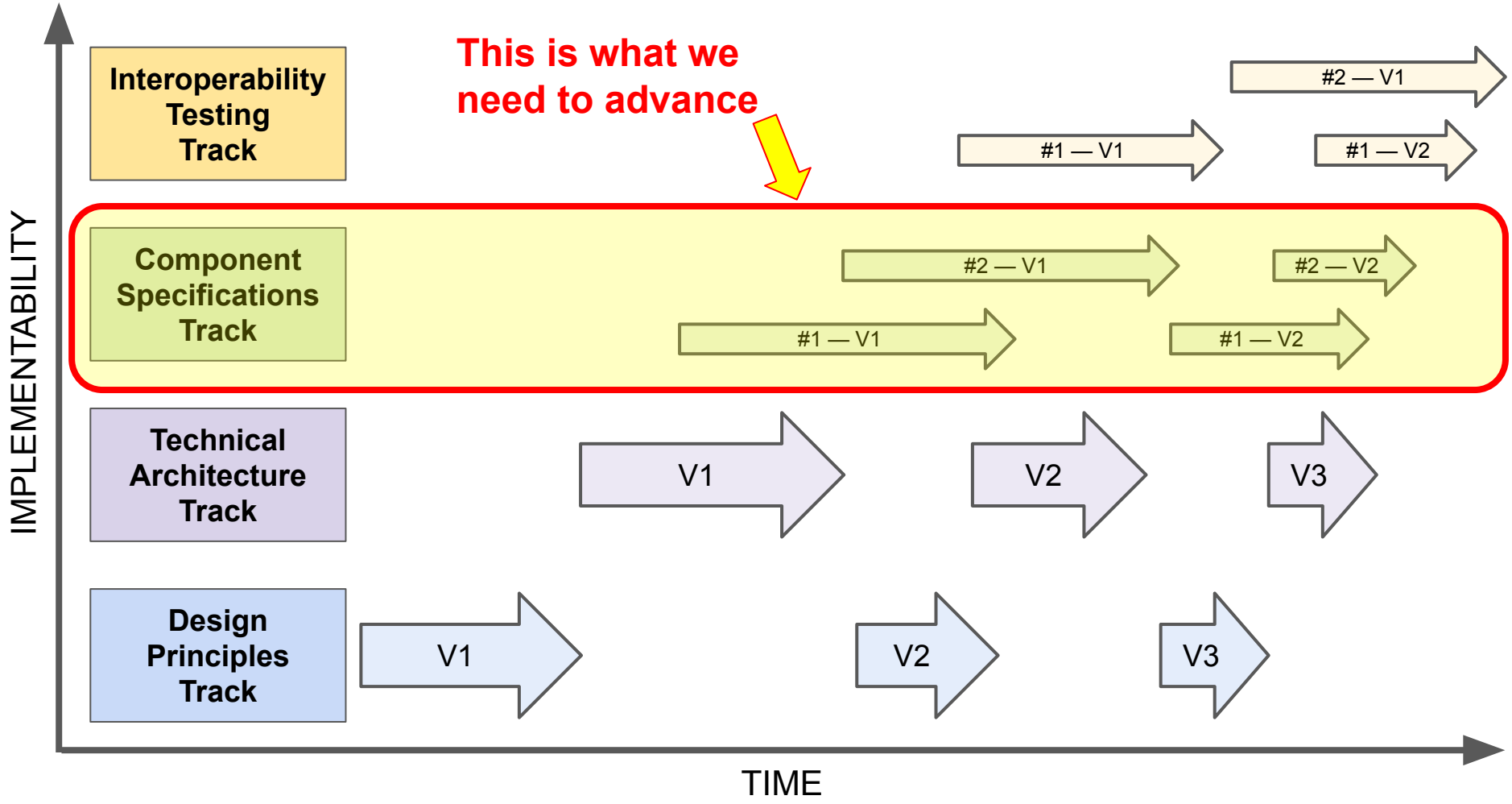
Open standard experts within Avast believe the planning and development of such a framework—designed to test commercial-grade implementations at scale—is **a two year project**.

So we need to make the commitment, assemble the resources, and start planning the effort **now**.

What will this require the Foundation to do?

Based on experience with similar interoperability certification frameworks (e.g., the OASIS STIX2Preferred (https://oasis-stixpreferred.org/) , Wifi Alliance (https://www.wi-fi.org/) Certifications), in broad strokes we will need to take the following three steps:

1. First, we will need to help advance the necessary **component specifications** at all four layers.
2. Second, as a Foundation will need to develop a **ToIP Interoperability Certification Framework** against which third parties can perform certification of implementations & use cases
    a. This framework will identify roles/Persona/Profiles of technology and how they may certify software acting as that persona
3. Third, one or more ToIP members will need to produce at least one Technology that matches at least one **ToIP Interoperability Profile**.


IMPLEMENTABILITY
TIME
Interoperability Testing Track
This is what we need to advance
#2 — V1
#1 — V1
#1 — V2
Component Specifications Track
#2 — V1
#2 — V2
#1 — V1
#1 — V2
Technical Architecture Track
V1
V2
V3
Design Principles Track
V1
V2
V3

Advancing component specifications

Which component specs will be mature enough when is not entirely in our control. Realistic candidates in a 2 yr time frame:

1. Layer 1 DID registry specs (both tech and governance)
2. Layer 2 wallet/agent specs (especially EU & Canada)
3. Layer 2 trust spanning protocol specs (DIDComm et al)
4. Layer 3 credential exchange specs (Aries, OIDC4VC, ISO)
5. Layer 4 UI/UX specs (FIDO, Secure QR codes, etc.)

The point is: ToIP members and our community as a whole can push to finish enough component specs to create at least one **full-stack interoperability profile**

Developing a ToIP Interoperability Certification Framework

- An important step is for the Foundation to publish our own ToIP Interoperability Certification Framework (TICF)
  - Defines roles/persona/profiles that fit into relevant use cases for interoperability
- **Critical for success**: Establishing a brand recognition of “ToIP Preferred” or similar **AND** ToIP must consider facilitating either:
  - **Option A**: Self-certification with published results/verification/reviews (similar to STIXPreferred, Wifi Alliance)
  - **Option B**: Certification lab funding or partner that agrees to act as certification lab based on TICF
- Depending on which option is chosen, define what additional resources, review boards, and infrastructure must be setup to support certifications
- The TICF specifies how certification is be performed, thus giving ToIP certification **a strong uniform meaning in the market—not just a document/framework to be ignored**

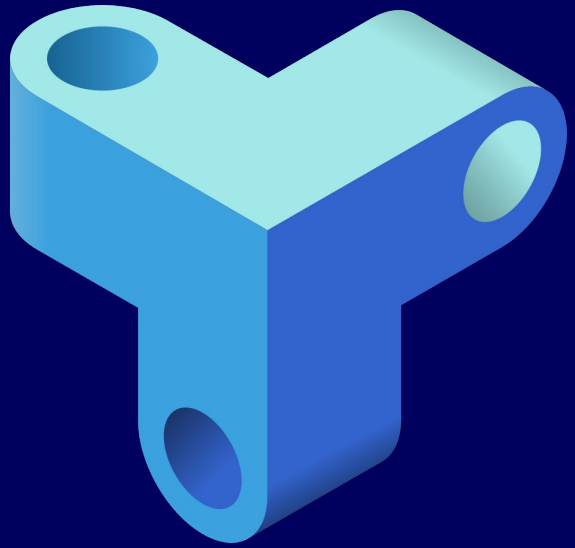
ToIP Interoperability Profiles

- In the early days of ToIP, Dan Gisolfi proposed that members start publishing ToIP interoperability profiles (“TIPs”) as quickly as possible
- That didn’t work because we hadn’t laid the proper foundation (our Design Principles and Technology Architecture Spec)
- We also didn’t have enough component specifications
- Once we have these, plus the TICF, we’re ready to establish one (or more) **TIP Working Groups** to develop one (or more) TIPs serving a specific set of digital trust ecosystems
- They should be driven by **groups of ToIP members who want to interoperate in a very publicly visible way**

First Step: Form a ToIP Interoperability Working Group

- A two year journey begins with the first step
- We propose that ToIP members who are serious about this strategic objective start the journey by forming a **ToIP Interoperability WG** (TIWG)
- The TIWG would hold a formation meeting in December, then start meeting monthly in January
- Task Forces would then form under the TIWG as needed (just as has been proven effective in other WGs)

Open Discussion



TRUST Over IP FOUNDATION