

Storage and Portability Task Force

Industry sector-agnostic

- [Overview](#)
- [Mission and Scope](#)
- [Intellectual Property Rights \(Copyright, Patent, Source Code\)](#)
- [Conveners](#)
- [Chairs](#)
- [Interested Members \(add your name and organization if you may be interested in joining this TF\)](#)
- [Objectives](#)
- [Technical components](#)
- [Example use case](#)
- [Deliverables](#)
- [Proposed schedule](#)
- [Shared documents and links](#)

Overview

Permanent and transient data stores will become an integral part of the [Dynamic Data Economy](#) (DDE), fostering user-centric consented privacy-preserving data access and safe and secure data sharing. In many instances, [Verifiable Credentials](#) (VCs) will be the payload authentication mechanism for bundled objects stored within transient containers. There will also be licensing and certification instances where VCs will be the only component required for the portability of form-based payloads. With storage and portability solutions being developed within a number of open communities, there is a need to ensure that all of those component solutions are interoperable across any network.

Mission and Scope

The mission of the *Storage & Portability Task Force* (SPTF) is to facilitate the creation of specifications and best practices for the interoperability of decentralized storage and portability components within the context of end-to-end Dynamic Data Economy (DDE) data flows. The scope of the SPTF will include all storage and portability component solutions (including data stores, hubs, containers and VCs) that are hosted at the Linux Foundation or external to it. Other working group activities will include creating template Requests for Proposal (RFPs) and additional guidance to utility and service providers regarding implementations in that capacity. The SPTF may organize Focus Groups to escalate the development of certain storage and portability components if deemed appropriate by the majority of the [Inputs and Semantics Working Group](#) (ISWG) members and in line with the overall mission of the ToIP Foundation..

Intellectual Property Rights (Copyright, Patent, Source Code)

This TF uses the same IPR licensing selections as the Inputs and Semantics WG:

- Copyright mode: [Creative Commons Attribution 4.0](#).
- Patent mode: W3C Mode (based on the [W3C Patent Policy](#)).
- Source code: [Apache 2.0](#).

Conveners

- [Christoph Fabianek](#) (OwnYourData)
- [Paul Knowles](#) (Human Colossus Foundation)

Chairs

- [Christoph Fabianek](#)

Interested Members (add your name and organization if you may be interested in joining this TF)

- [Paul Knowles](#)
- [Robert Mitwicki](#)
- [Philippe Page](#)
- [Amar Tumballi](#) (Dhiway)
- [Ken Adler](#) | ThoughtWorks
- [John Walker](#) | CCI

Objectives

The objectives of the SPTF are:

- To create specifications, white papers and other educational resources that provide enhanced insight on topics related to storage and portability, including:
 - Enhancements to existing or pipeline components to enable full interoperability within DDE data flows;

- Defining and introducing digital solutions to help prevent unauthorized access to data payloads contained in (or resulting from) any data store, hub, container or VC;
 - Describing digital watermarking techniques to determine unauthorized data sharing.
- To introduce linking identifiers as a common threading mechanism for linking information across a number of container-held profiles and datasets for the purpose of data revocation;
- To introduce any necessary controls to better enable:
 - Authorized data access;
 - Safe and secure data sharing; and
 - Authentic data flows.
- To establish a ToIP liaison group for other standards bodies involved in the management and assessment of decentralized storage and/or portability components.

Technical components

The SPTF will build upon the core components of the ISWG, with special emphasis on:

- Permanent storage components (personal private key-access data stores, vaults and hubs);
- Transient storage components (permissioned token-access pods and containers);
- Verifiable Credentials (VCs) as a mechanism for (i.) storage payload authentication and (ii.) portability of form-based payloads.

Example use case

- Digital Immunization Passport
 - (i.) Enabling data interoperability and compatibility by establishing interfaces between health industry stakeholders and individuals while progressing standardized interfaces for personal data stores (PDSs);
 - (ii.) Addressing data transparency issues through Usage Policies and data provenance in transient containers (e.g. Semantic Containers);
 - (iii.) Addressing security/privacy issues through blockchain technology and digital watermarking on shared data payloads.

Deliverables

Proposed schedule

[Meeting information](#)

Shared documents and links

- Semantic Containers (OwnYourData) - <https://www.ownyourdata.eu/en/semcon/>
- Personal Data Stores [Data Vaults] (OwnYourData) - <https://data-vault.eu>
- Confidential Storage 0.1 (DIF) - <https://identity.foundation/confidential-storage/>
- Solid Pods (Solid/Inrupt) - <https://solidproject.org/users/get-a-pod>
- Verifiable Credentials Data Model 1.0 (W3C) - <https://www.w3.org/TR/vc-data-model/>
- OpenDSU (OpenDSU Project) - <https://opensu.com/?Specifications/rfc001.html>