Working Group Charter

This Working Group Charter establishes the Scope and intellectual property terms used to develop the materials identified in this Working Group Charter for the Project. Only Project Steering Members, Associates, and Contributors, as applicable, that have executed this Working Group Charter will be bound by its terms and be permitted to participate in this Working Group.

1. Working Group Name. **Secure Data Storage Working Group**

2. Working Group Scope.

   Create one or more specifications to establish a foundational layer for secure data storage (including personal data), specifically data models for storage and transport, syntax, data at rest protection, CRUD API, access control, synchronization, and at least a minimum viable HTTP-based interface compatible with W3C DIDs/VCs.

   The Identity Hubs and Encrypted Data Vaults documents will be used as a use case, requirements, and technical input for the collaborative effort.

The Working Group will:

- Gather and document use cases and requirements from stakeholders,
- Design a data model and one or more representations for encrypted storage and transport,
- Design a cryptographic security architecture that protects information in transit and at rest, noting that different approaches may be taken for information in transit and information at rest and bearing in mind potential quantum computing attacks,
- Design an API that enables a remote system to interact with the data,
- Design or identify at least one access control architecture for the API,
- Develop the necessary implementation(s) to validate the viability of the specifications,
- Design or identify a data synchronization and replication protocol, to ensure user data is portable.
- Discuss and implement an encrypted indexing and search mechanism that prevents a storage provider from mining customer data and metadata,
- Consider how the design of the HTTP-based interface will affect the communication protocol for non-HTTP-based APIs,
- Strive to utilize existing standards when possible, and
- Focus on an HTTP-based interface for the API mechanism.

Out of Scope

- Design or development of DID Methods or Verifiable Credentials.
- Design or development of new data transfer protocols (e.g., HTTP, QUIC).
- Invention of new cryptographic algorithms for encryption, signing, or hashing.
- Design or development of database or ledger systems such as blockchains.
- Invention of new mechanisms for Authentication or Authorization (i.e., do not use mechanisms that are not standardized or not work items of the W3C CCG, DIF, or existing standards WG).
- Invention of new mechanisms for querying or inserting data (e.g., SQL, or Gremlin) (i.e., do not use mechanisms that are not standardized or not work items of the W3C CCG, DIF, or existing standards WG).
- Design or development of non-HTTP based APIs (e.g., APIs over Bluetooth, UDP, or NFC).

3. Copyright Policy. Each Working Group must specify the copyright mode under which it will operate prior to initiating any work on any Draft Deliverable or Approved Deliverable other than source code. The copyright mode for this Working Group is.

   - Creative Commons Attribution 4.0, as set forth in Appendix A,
     .

4. Approved Deliverable Patent Licensing. Each Working Group must specify the patent mode under which it will operate prior to initiating any work on any Draft Deliverable or Approved Deliverable other than source code. The patent mode for this Working Group is:

   - W3C Mode, as set forth in Appendix A,

The assurances provided in the selected patent mode are binding on the Working Group Participant's successors-in-interest. In addition, each Working Group Participant will include in any documents transferring ownership of patents subject to the assurance provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

5. Source Code. Working Group Participants contributing source code to this Working Group agree that those source code contributions are subject to the Developer Certificate of Origin version 1.1, available at http://developercertificate.org/, and the license indicated below. Source code may not be a required element of an Approved Deliverable specification.
   - Apache 2.0, available at http://www.apache.org/licenses/LICENSE-2.0.html.
6. Non-Working Group Participant Feedback and Participation. Upon the Approval of the Working Group Participants, the Working Group can request feedback from and/or allow Non-Working Group Participant participation in a Working Group, subject to each Non-Working Group Participant executing the Feedback Agreement set forth in DIF Feedback Agreement

By the Project

Signature:	
Print Name:	
Title:	
Company Name:	Decentralized Identity Foundation
Email:	
Address:	1 Letterman Drive Building D, Suite D4700 San Francisco, CA 94129
Date:	

By the Steering Member/Associate/Contributor

Signature	
Print Name:	
Title:	
Company Name:	
Email:	
Address:	
Date:	