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 that Joined the Working Group will be bound by its terms and be permitted to participate in this Working Group.

1. Working Group Name. **Applied Cryptography Working Group**

2. Working Group Scope.

   The Cryptography Working Group will explore cryptographic protocols and -primitives related to Decentralized Identity, including, but not limited to, specific and actual cryptographic topics, such as BBS+ signatures and revocation strategies, as well as signature suites and encryption.
   The working group will define focus topics, create cryptographic protocols, and choose the underlying cryptographic primitives for them.

   The Working Group will:

   - Define focus topics with input from the Decentralized Identity community based on other standardization activities.
   - Discuss, evaluate, suggest and describe cryptographic protocols and their underlying cryptographic primitives as a baseline for implementation.
   - Handle the registration (e.g., with IANA) of items like new cryptographic protocols, key and curve types.
   - Discuss various cryptographic techniques that have applications to Decentralized Identity use-cases, more specifically on the topics of:
     - Group signature schemes.
     - Multi-message signature schemes supporting selective disclosure/reveal.
     - Non-correlating revocation signature mechanisms.
     - Privacy-preserving signature binding mechanisms.
     - Predicate techniques for Verifiable Credentials and other uses.
     - Other topics as determined by the working group.
   - Draft standards-track and other documents describing the use of these cryptographic protocols and their underlying primitives.
   - Export group output to various standards bodies for further development and standardization, such as the IETF CFRG.
   - Provide a forum for implementers to give feedback on the implementability of the cryptographic protocols that are documented by the working group.
   - Supply and maintain relevant test vectors associated with the documented cryptographic techniques.

   Out of Scope

   - The invention of new cryptographic primitives, such as defining new cryptographic curves or curve operations.
   - Implementation of cryptographic primitives and cryptographic protocols.
   - Test Suites for group-defined protocols, beyond a set of test vectors.

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, Copyright Policy Option 2.

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, Patent Policy Option 4.

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. Please contact the Executive Director for a copy of the DIF Feedback Agreement.

By the Project

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

By the Steering Member/Associate/Contributor

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