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. **Wallet Security WG**
2. Working Group Scope.

2.1. The Working Group will:

A. Define a common terminology for understanding the security requirements applicable to wallet architectures and wallet-to-wallet and wallet-to-issuer/verifier protocols.

B. Classify, specify and describe security architectures common to wallets(risks, motivation, etc..)

- Scope on different architectures (native apps, multi-edged/device and pure web-based wallet)
- potentially design reference model for each wallet security architecture
- author recommendations or interoperability profiles based on existing regulatory frameworks, mandates and specifications for wallet capabilities
- Scope on different types of data subjects and wallet controllers (individuals, legal persons, teams), including IoT “Wallets” (will be described in further details)

C. Review and leverage wallet security-relevant aspects of prior art, including normative specifications (e.g. Universal Wallet (W3C-CCG)), implementation guidance (e.g. VC EDU (W3C-CCG)), and reference implementations (e.g. Learner Wallet project (T3))

- Interface with other DIF and DIF-affiliated WGs to understand how wallet-to-wallet and wallet-to-issuer/verifier protocols can be used to communicate security capabilities and guarantees

D. Produce guidelines for how to classify and specify the security capabilities of verifiable-credential wallets such as key management, credential storage, device-binding, credential exchange, backup, recovery, and portability of wallets. These guidelines may include most or all of the following:

- Key management requirements and assess interoperability with existing KMS specifications (such as CCG webKMS and Aries DKMS)
- Backup and recovery requirements for the wallet and data stored in it.
- Wallet storage requirements
- Provable wallet security assertion methods
- Analyze how user/wallet authentication capabilities(including biometric security) can or should map to level of assurances.

- Analyze bindings between individuals, identifiers, wallets, devices, and/or documents/data (e.g. biometric enrolment assumptions)
- Analyze how consent guidelines (in the legal, UX, wallet-specific parts of holder-verifier and holder-issuer trust relationship and data-management senses) can or should map to security assumptions
- Prepare security impact assessment of custodial management, guardianship, agency, delegation

E. Map related wallet security mechanisms to assurance levels, e.g. with explicit reference to regulatory frameworks

- Identify potential attack vectors and risks

F. Analyze and make recommendations on how to work within attestation and verification frameworks for wallet security according to current regulations(auditing of the wallet implementation), including cases where these apply to wallet implementation (product quality) and/or wallet deployment (service quality) (i.e. web-hosted wallets).

2.2. Principles:

A. The security group will identify the security capabilities of digital wallets that implementers and trust frameworks can choose to include. These security capabilities will vary in security level, from moderate to very high, and include topics such as key management, credential storage, device-binding, credential transport protocols, backup, recovery, consent, and portability of wallets. Implementers and trust frameworks will choose to include or exclude these higher-level functional capabilities depending on their required security posture.

B. Focus primarily on guidance and Best Current Practices documents. Any interface- and protocol-specific implementation details will be in appendices of the specifications, and MAY be prepared by subsets of the group in separate work items (e.g. implications of CHAPI, DIDComm, SIOP, and other communication protocols for wallet design and compliance)

2.3. Tentative work plan of deliverables:

A. Deep diveon common terminology and wallet-security related aspects of prior art, and wallet architecture (first work item)
B. Guidelines on security capabilities such as key management, storage, back-up, recovery, device-binding, consent, and custodial management (ongoing/iterative)
C. Mapping of wallet security mechanisms according to assurance levels and identify potential attack vectors and risks
D. Solicit Implementer's Reports or other structured feedback from wallet implementers
E. Paper on Best Practices of interactions between wallets of different security capabilities (synthesizing or summarizing other deliverables)

2.4. Out of Scope:

A. Explicit Wallet implementations
B. Explicit mandatory security mechanisms, signatures schemes or other
C. Explicit mandatory regulatory framework compliance
D. Explicit full certification requirements lists or certification paths
E. Defining secure messaging protocols
F. Defining new protocols for holder authentication, and exchange of verifiable credentials/presentations
G. Defining PKI models or other key management schemes
H. Develop new security mechanisms

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:

□ Copyright Grant to Project, as set forth in Appendix A, Copyright Policy Option 1.

X Creative Commons Attribution 4.0, as set forth in Appendix A, Copyright Policy Option 2.

□ Open Web Foundation 1.0. (only for those Working Groups selecting the Open Web Foundation mode for patent licensing).

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:

□ RAND Royalty-Free Mode, as set forth in Appendix A, Patent Policy Option 1.

□ International Mode, as set forth in Appendix A, Patent Policy Option 2.

□ Open Web Foundation Agreement 1.0 Mode, as set forth in Appendix A, Patent Policy Option 3.

X W3C Mode, as set forth in Appendix A, Patent Policy Option 4.

□ No Patent License. No patent licenses are granted for the Draft Deliverables or Approved Deliverables developed by this Working Group.

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.

X Apache 2.0, available at http://www.apache.org/licenses/LICENSE-2.0.html.

□ MIT License, available at https://opensource.org/licenses/MIT.

□ Mozilla Public License 2.0, available at https://www.mozilla.org/MPL/2.0/.

□ Other. _____

□ No source code will be developed.

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.
7. By executing this Membership Agreement, I agree to be bound by this Membership Agreement, the Project Charter, and the terms of the Working Groups I Join.

By the Project

Signature:	
Print Name:	
Title:	Executive Director
Company Name:	**Decentralized Identity Foundation**
Email:	
Address:	
Date:	

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