Request for Proposal (RFP):
ISO/IEC 17065 Accreditation Consultancy

Project Scope: FIDO Alliance Wallet and Authenticator Certification Schemes
Proposed Start: July-August 2026 | **Target Completion:** Q2 2027

1. Project Overview

About FIDO Alliance

The FIDO Alliance (www.fidoalliance.org) enables identity technologies that put trust and simplicity at the center of interactions among people, services, and devices.

The Alliance provides a member-driven forum that focuses on:

1. **Technical Specifications:** Creating open, scalable, and interoperable mechanisms to enable simple, secure, privacy-preserving identity technologies, such as phishing-resistant user authentication with passkeys.
2. **Certification Programs:** Developing and managing industry certification programs to ensure the successful worldwide implementation of its specifications and globally-recognized performance criteria.
3. **Education and Market Adoption Programs:** Implementing educational and market adoption initiatives to promote its standards and certifications globally.

Scope Statement

FIDO Alliance is seeking a specialized consulting partner to guide us through the ISO/IEC 17065 accreditation process. Our objective is to be recognized as a Certification Body (CB) capable of evaluating and certifying wallet components, including authenticator sub-components, under the **FIDO Alliance Wallet and Authenticator Certification Schemes**.

This engagement will cover three primary outcomes, including a framework of deliverables.

1. Conduct a comprehensive readiness review of the certification body's remote-only operating model to ensure compliance with ISO/IEC 17065, accreditation requirements, and regulatory expectations.

   Key assessment considerations to include, but not limited to:

   - **Confidentiality and Information Protection Controls** – Document and validate policies, procedures, and technical safeguards that protect confidential certification information, applicant data, evaluation evidence, and certification records in a distributed work environment.
   - **Secure Records Management** – Establish and verify controls for the creation, storage, retention, backup, retrieval, and disposal of certification records, ensuring integrity, traceability, and controlled access.
   - **Access Control Framework** – Implement and document role-based access controls, authorization procedures, user provisioning and deprovisioning processes, authentication requirements, and periodic access reviews for all certification systems and repositories.
   - **Remote Impartiality Committee Operations** – Develop procedures and evidence demonstrating the effective operation of the Impartiality Committee in a virtual environment, including meeting management, conflict-of-interest controls, participation requirements, decision recording, and maintenance of impartiality.
   - **Controlled Certification Decision Process** – Establish documented controls ensuring certification decisions are independently reviewed, appropriately authorized, traceable, and protected from undue influence within a remote operating model.
   - **Evaluator Access to Evidence and Systems** – Define secure processes that enable evaluators, technical reviewers, and decision-makers to access evaluation evidence, technical documentation, and certification records while maintaining confidentiality and integrity requirements.
   - **Assessment and Accreditation Readiness** – Demonstrate the organization's ability to support remote and on-site assessments conducted by accreditation bodies and

regulators, including the provision of records, personnel interviews, witness activities, and evidence reviews.

- **Time Zone and Availability Planning** – Document operational procedures and staffing commitments that ensure timely support and availability for European accreditation bodies, National Accreditation Bodies (NABs), assessors, and stakeholders despite Pacific Time-based operations.
- **Business Continuity for Distributed Operations** – Develop and maintain procedures that ensure continuity of certification activities, decision-making, records access, and stakeholder communications during personnel absences, technical outages, or other operational disruptions.

2. Assess and evaluate whether and how best this accreditation scope may support certification activities for European Digital Identity Wallet solutions.

3. Following the first outcome, transition from the initial setup to a successful accreditation decision by an applicable EU-based Accreditation Body (Appointed under Regulation (EC) No 765/2008) specifically for the FIDO scope.

   Key deliverables include, but are not limited to:

   - **Competence Framework and Role Matrix** – Develop and maintain a documented competence matrix for all personnel performing certification activities under ISO/IEC 17065, including:
     - Application Reviewers
     - Evaluation Planning Personnel
     - Evaluators/Assessors
     - Technical Reviewers
     - Certification Decision-Makers
     - Surveillance and Maintenance Reviewers
     - Complaints and Appeals Handlers
     - Impartiality Committee Members
   - **Qualification Records and Personnel Files** – Establish and maintain qualification records for each individual performing certification functions, including education, training, technical expertise, certifications, work experience, competency assessments, authorizations, and ongoing professional development activities.
   - **Role-Specific Competency Criteria** – Define and document role-specific competence requirements, including technical, certification, regulatory, and program-specific knowledge where applicable (e.g., ISO/IEC 17065, ISO/IEC 17025, biometric evaluation methodologies, identity verification technologies, FIDO certification programs,

cybersecurity requirements, and applicable standards).

- **Competency Assessment and Authorization Process** – Implement procedures for initial qualification, competency evaluation, authorization, periodic reassessment, and continued approval of personnel performing certification activities.
- **Training and Professional Development Program** – Develop a training framework and records system to ensure personnel maintain competence as certification requirements, standards, technologies, and accreditation obligations evolve.
- **Audit-Ready Competence Documentation** – Provide complete, traceable, and accreditation-ready evidence demonstrating that all personnel assigned to certification activities meet documented competence and impartiality requirements.

2. Scope of Work (SOW)

The consultant will be responsible for assessing, developing, and aligning our Quality Management System (QMS) with both ISO 17065 and the FIDO Alliance Certification Policies, demonstrating the ability to conduct evaluations against critical reference standards applicable to the components under evaluation.

[Appendix A: Reference Standards, Schemes, Policies]

- **Work Stream A: FIDO-Specific Gap Analysis**
  - Audit current technical capabilities against functional and security requirements for authenticator (Level 1 to L3+) and wallet components.
  - Map the FIDO "Certification Program/Certification Secretariat" workflows to ISO 17065 process requirements.
  - After the gap analysis is complete, the scope will be re-evaluated based on its findings.

- **Work Stream B: Impartiality & Governance**
  - Support in improving the Board Certification Committee (acting as the Impartiality Committee) with specific expertise in the cybersecurity, authentication, identity, and certification industries.
  - Develop a conflict of interest and decision independence framework, including implementing policies, procedures, and controls to ensure impartiality and independence between evaluation, testing, review, and certification decision-making activities. Define role separation requirements, including eligibility and exclusion criteria for evaluators, technical reviewers, certification decision-makers, and other personnel involved in the certification process (e.g., FIDO Certification Staff, FIDO Accredited Laboratories). Establish conflict-of-interest declaration and management procedures, restrictions on personnel involved in testing, consulting, or advisory activities, and documented safeguards

demonstrating that certification decisions are made independently of evaluation activities. Provide objective evidence and records sufficient to demonstrate impartiality and decision independence during accreditation assessments and audits.
    - Develop a personnel competence framework, including a competency matrix, qualification records, and authorization criteria for all ISO/IEC 17065 functions, including application review, evaluation planning, evaluation, technical review, certification decision-making, surveillance, complaints and appeals handling, and impartiality committee participation.
    - Establish policies and procedures governing the use of subcontracted evaluation resources, including ISO/IEC 17025 testing laboratories and, where applicable, ISO/IEC 17021-1 audit bodies, ensuring appropriate oversight, competence, impartiality, and confidentiality controls while preserving the certification body's ultimate responsibility for certification outcomes and independent certification decisions.

- **Work Stream C: Documenting ISO/IEC 17065 Procedures and Manuals to the FIDO Schemes**
    - Assess current Quality Manuals and SOPs for the intake, evaluation, and certification of FIDO Authenticators, based on the findings from the gap analysis.
    - Develop and deliver a complete, accreditation-ready certification scheme package, including scheme scope, certification objects, normative requirements, evaluation methodology, sampling rules, review and decision criteria, certification outputs, surveillance and maintenance processes, recertification requirements, suspension and withdrawal procedures, and documented alignment with ISO/IEC 17067 scheme types, including Type 6 certification model requirements where EUDIW readiness assessments are included.
    - Develop and deliver lifecycle and post-certification control procedures, including surveillance programs, random testing and inspections, recertification, change impact analysis, vulnerability notification and handling, special evaluations, certification maintenance, suspension, restoration, and withdrawal/cancellation processes, complaints and appeals management, record retention, information protection controls, and public certificate and certification report templates.
    - Develop one or more Certification and 3rd-party (e.g., FIDO Accredited Laboratories) Agreement templates that comply with both FIDO Alliance requirements and ISO standards.

- **Work Stream D: Pilot Certification & Evidence Generation**
    - Conduct one or more, end-to-end mock certification demonstration from intake through certification issuance and surveillance planning, generating a complete accreditation-ready certification file that includes application review, contract review, evaluation planning, evaluator competence records, evidence sampling and assessment records, laboratory and evaluation reports, technical review records, certification decision documentation,

nonconformity and corrective action records, certificate issuance records, public certification outputs, surveillance planning, and certification maintenance documentation.
    - Ensure all records—from Functional Test results to Security Evaluation reports—are structured for Accreditation Body (AB) review.
    - Develop and deliver a comprehensive evaluation methodology and assessment framework, including application review, evaluation planning, evidence collection and sampling, control-to-component traceability, EUDIW risk-register coverage mapping, dependency analysis, functional testing, architecture review, source code and design review (where applicable), vulnerability assessment, evidence reuse criteria, technical review procedures, and certification decision inputs.
    - Generate representative certification records, evaluation reports, technical review records, certification decisions, certificates, and supporting evidence packages suitable for accreditation assessment and ongoing certification operations.
    - Validate the effectiveness of the certification scheme, quality management system, and operational procedures through pilot evaluations and documented lessons learned.

- **Work Stream E: External Assessment Support**
    - Support Accreditation Body (AB) selection, engagement, application, and assessment planning activities.
    - Conduct a mandatory Internal Audit and Management Review prior to Accreditation Body assessment activities, including identification, documentation, and closure of nonconformities and corrective actions.
    - Provide on-call technical and procedural support during Accreditation Body document reviews, office assessments, and witness assessments of FIDO certification activities.
    - Accreditation Readiness and Assessment Preparation – Prepare the organization for practical accreditation readiness beyond procedural compliance. Deliver all documentation, records, templates, and objective evidence necessary to support a successful ISO/IEC 17065 accreditation assessment, including:
        - Accreditation scope and scope statement
        - Certification scheme files and ISO/IEC 17067 mappings
        - Process maps and certification workflow documentation
        - Personnel competence matrices, qualification records, and authorization records
        - Impartiality risk assessments and conflict-of-interest controls
        - Subcontractor qualification, monitoring, and oversight records
        - Certification review and decision-making rules
        - Certification file templates and records management procedures
        - Certificate, certification report, and public reporting templates
        - Surveillance, recertification, and certification maintenance procedures
        - Vulnerability notification, change management, and special evaluation

procedures
        - Record retention, confidentiality, and information protection controls
        - Complaints, appeals, and dispute resolution procedures
        - Internal audit, management review, CAPA, and continual improvement records
        - Complete mock certification files and accreditation evidence packages and
        - Preparation for Accreditation Body document reviews, office assessments, and witness assessments, including assessor interview preparation and evidence traceability demonstrations
    - Witness Assessment Readiness Demonstration – Develop and execute a mock Accreditation Body document review and witness assessment exercise to validate the organization's readiness to demonstrate conformity with ISO/IEC 17065 requirements and defend certification decisions, records, competence assignments, and certification scheme implementation during accreditation assessment.

- **Work Stream F: Accreditation Readiness Dossier & Pre-Assessment Preparation**
    - Develop and deliver a complete accreditation-ready documentation package, including certification scheme files, accreditation scope documentation, process maps, governance and impartiality controls, personnel competence records, subcontractor oversight records, certification decision rules, and all required ISO/IEC 17065 policies, procedures, templates, and supporting records.
    - Establish and validate end-to-end certification operations, including evaluation methodologies, certification lifecycle controls, surveillance and recertification processes, vulnerability and change management procedures, complaints and appeals handling, public certification reporting, and production of complete sample certification files and accreditation evidence packages.
    - Conduct and document organizational readiness activities, including internal audits, management reviews, CAPA processes, mock certifications, mock Accreditation Body document reviews, readiness assessments, and remediation of identified gaps.
    - Prepare and support Accreditation Body engagement activities, including accreditation scope validation, pre-application meetings, assessment planning, witness assessment preparation, assessor interview readiness, evidence traceability demonstrations, and on-call support through accreditation assessment and witness audit activities.

3. Proposed Timeline (July 2026 - June 2027)

This timeline is designed to meet the **Q2 2027** accreditation goal.

Phase	Timeframe	Key Milestones
I. Discovery	July – Aug 2026	**Project Kick-off**; Gap Analysis; FIDO Scheme Mapping.
II. Development	Sept – Nov 2026	Drafting and establishing QMS, certification procedures, subcontracting rules, surveillance procedures, scheme-interface documentation, and the certification decision process; setting up the Impartiality Committee.
III. Training	Dec 2026	Staff training on FIDO Security Levels and ISO 17065.
IV. Pilot Ops	Jan – Feb 2027	Execution of a "Mock" FIDO Certification; Internal Audit. Resolution of non-conformities.
V. Pre-Application	March 2027	Review accreditation scope, scheme documentation, witness assessment approach, assessment logistics, evidence expectations, and application readiness before formal submission.
VI. Application	March 2027	Formal application to Accreditation Body (NAB).
VII. Assessment	April – May 2027	AB Document Review and On-site/Witness Assessment.
VIII. Decision	June 2027	Closure of non-conformities; **Accreditation Granted.**

4. Consultant Qualifications

Bidders must demonstrate:

- **Proven ISO 17065 Success:** A portfolio of clients who have achieved accreditation in the cybersecurity or hardware security domain.
- **Technical Bench:** Access to experts who understand cryptographic modules, TEE (Trusted

Execution Environments), and Biometric requirements.

- **Certification Schemes:** Familiarity with well-known certification schemes, including Common Criteria, Protection Profiles, and cryptographic mechanisms.
- **Authentication and Identity:** Background in authentication and identity protocols is a plus for this engagement.
- **Regulatory Compliance:** Familiarity with Regulation (EU) 2024/1183, Implementing Regulation (EU) 2024/2981, Article 5a/5c requirements, EUDI Wallet Architecture and Reference Framework, national EUDIW certification schemes, EUCC, WSCA/WSCD, assurance level high under eIDAS, dependency analysis, data protection evaluation, and vulnerability assessment against high attack potential.
- **Certification Experience:** Demonstrated ability to meet affiliated ISO accreditations (i.e., ISO/IEC 27001, ISO/IEC 17065, ISO/IEC 17025).
- **Accreditation Body Experience:** Demonstrated experience and knowledge of EU-based Accreditation Bodies.

5. Proposal Submission Requirements

Please provide proposals in writing to karen@fidoalliance.org and paul@fidoalliance.org by June 29th, 2026. A decision will be made by July 10th, 2026.

Proposals should include the following:

1. **Technical Methodology:** How will you ensure that FIDO Alliance's certification operations, evaluation methodologies, and management system meet the functional, security, and accreditation requirements applicable to FIDO certification programs under ISO/IEC 17065? Please describe your methodology, implementation approach, and accreditation strategy, including how you will develop both the Quality Management System (QMS) and the practical accreditation-readiness package required for successful accreditation. Your response should address the development and validation of accreditation scope documentation, certification scheme files, process maps, competence matrices, impartiality analyses, subcontractor qualification frameworks, certification decision rules, complete mock certification files, surveillance, vulnerability management, and change-management procedures, CAPA processes, mock assessments, witness-assessment readiness, and other objective evidence required to demonstrate operational readiness to an Accreditation Body.
2. **Case Study:** Two (2) examples of similar accreditation projects in the identity or security space.
3. **Examples:** Provide examples of how deliverables for gap analysis, documentation, and reports will be formatted, along with an explanation of how you conduct projects and personnel who will be involved in each phase.
4. **Risk Mitigation Plan:** How you will ensure the tight 12-month timeline is met despite potential

AB scheduling delays.

5. **Cost Proposal:** Proposals based on a time-and-materials model. Please structure the bids by the phases in Section 2. Bids should include:
    - **Labor:**
        - Estimate of hours and associated costs for each phase, including the hourly rate,
        - Number of and role of personnel involved.
    - **Materials and Expenses:**
        - Materials and any associated markups.
        - Additional expenses associated with the delivery of the scope of this RFP, with any associated markups.
    - **Not-to-exceed Cap:**
        - Proposals must include a not-to-exceed maximum.

6. Evaluation Criteria

Proposals will be evaluated based on the following:

1. **Experience**
    - Previous experience with ISO 17065.
    - Examples provided as part of the RFP.
2. **Key Personnel**
    - Qualifications and skills of key personnel are proposed.
    - Ability to meet remotely and support efforts in the client's time zone (Pacific).
3. **Cost**
    - The RFP will be reviewed for cost-effectiveness and competitive hourly rates.
4. **Proposed Approach**
    - Completeness of proposal.
    - Structure of approach and methodology.
    - Proposal matches the scope of the RFP.
5. **Accreditation Readiness Strategy**
    - Quality and practicality of the proposed accreditation-readiness approach, including preparation of accreditation scope documentation, certification scheme files, and supporting accreditation evidence.
    - Approach to personnel competence management, impartiality controls, certification decision independence, and subcontractor qualification and oversight.
    - Methodology for developing mock certification files, accreditation evidence packages, and other records required to demonstrate operational readiness.
    - Quality of the proposed pre-assessment, CAPA, Accreditation Body engagement, and witness-assessment preparation strategy.

- Demonstrated understanding of the distinction between ISO/IEC 17065 documentation development and the practical activities required to achieve successful accreditation.

Appendix A

Industry Standards and Requirements

- W3C WebAuthn
- FIDO CTAP
- FIDO UAF
- FIDO Security Requirements
- Common Criteria CC:2022 / EUCC HIGH level - for secure elements, SE apps, and high-assurance components WSCA/WSCD
- FITCEM (EN 17640) and/or EUCC - Substantial level: for the Wallet app/instance. - Not sure if this will be applicable for the HSM on the server use case as well.
- ENISA ECCG Agreed Cryptographic Mechanisms (à la FIPS 140-3)
- Organizational / Management standards
    - ISO/IEC 27001 (Information Security)
    - ISO/IEC 9001 (Quality Management)
- ETSI family standards
    - EN 419 241-1 (Protection Profiles for QSCDs)
    - EN 319 401 (General Policy Requirements for TSPs)
    - EN 319 403-1 (Requirements for Conformity Assessment Bodies)
    - EN 319 411-1 / -2 (Policy & security for TSPs issuing certificates)
    - EN 319 421 (Time-stamping)
    - EN 319 521 (Remote QSCD)
    - TS 119 403-2 / -3 (Audit & accreditation for eIDAS)
    - TS 119 431-1 (Electronic Registered Delivery Services)
    - TS 119 441 (Policy & security for eSeals)
    - TS 119 495 (Qualified certificates for electronic signatures/seals)
    - TS 119 461 (Identity proofing of trust-service subjects)
- ISO/IEC 18013-5
- ISO/IEC 18013-7
- ISO/IEC DTR 25219
- OpenID4VP
- OpenID4VCI
- Digital Credentials API
- Credential data structures (ISO MDOC, SD-JWT, and Longfellow ZKP models)

EUDIW Legal and Certification Framework

- Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183
- Commission Implementing Regulation (EU) 2024/2981 on certification of European Digital

Identity Wallets
- Commission Implementing Regulation (EU) 2024/2979 on integrity and core functionalities
- Commission Implementing Regulation (EU) 2024/2982 on protocols and interfaces
- Commission Implementing Regulation (EU) 2024/2977 on person identification data and electronic attestations of attributes
- Commission Implementing Regulation (EU) 2024/2980 on notifications to the Commission concerning the EUDI Wallet ecosystem
- Applicable national EUDIW certification schemes and scheme-owner rules
- EN ISO/IEC 17067:2013, type 6 certification scheme requirements

Lifecycle, Vulnerability, and Surveillance References

- EN ISO/IEC 30111:2019 vulnerability handling processes
- Cyber Resilience Act Annex I vulnerability handling requirements, where applicable
- EUDIW national certification scheme requirements for surveillance, maintenance, vulnerability disclosure, suspension, cancellation, and recertification
- Evidence requirements for version management, update management, vulnerability management, and dependency analysis