## 1. Project Description

The Zcash Community Grants (ZCG) committee is inviting qualified individuals or companies (Grantee(s)) to submit a proposal to extend the Zcash memo field to enable secure messaging for the Zcash community. The current memo field in Zcash lacks several essential features necessary for secure messaging, such as being signed to verify the origin of messages and being forward-secure to protect against future key compromises. The project will address these issues by developing a reference implementation of a secure messaging application built on top of the extended memo field and a ZIP proposal to support the inclusion of these changes in a future Zcash network upgrade. The project will include a thorough security analysis of the extended memo field and the reference implementation, as well as user documentation for the reference implementation. The project deliverables will include a detailed design document outlining the proposed extension of the memo field, a ZIP proposal for the inclusion of the extension in a future Zcash network upgrade, implementation of the extended memo field and reference implementation, security analysis, and user documentation.

The relationship between the winning Grantee(s) and ZCG shall be that of a grantee and grantor, governed by standard grant terms and conditions.

## 2. Project Assumptions

The following assumptions were made in the development of this Scope of Work:

- The Zcash network will support the extended memo field and the proposed network upgrade.
- The Zcash community will support the ZIP proposal and its inclusion in a future network upgrade.
- The reference implementation of the secure messaging application will be built on top of the Zcash network and will utilize the extended memo field.
- The reference implementation will meet the needs of typical users for secure messaging and will be user-friendly.
- The security analysis will identify any potential vulnerabilities in the extended memo field and the reference implementation and provide recommendations for addressing them.
- The implementation of the extended memo field and the reference implementation of the secure messaging application will be completed within the proposed timeline.
- The reference implementation will be well-documented and easy to understand for users and developers.
- The team will have the necessary experience and qualifications to complete the project successfully.

## 3. Scope of Work

Problem statement:

- The memo field in Zcash is currently lacking several features necessary for secure messaging, making it difficult to verify the origin of messages and protect against future key compromises. The goal of this project is to extend the memo field with additional features to enable the creation of secure messaging applications with Signal-like security properties.

Project goals and Required Elements:

a. The goal of this project is to extend the Zcash memo field to support secure messaging by:
    i. Signing the memo field to enable verification of the origin of messages.
    ii. Implementing forward-security for the memo field to protect against future key compromises.
    iii. Developing a ZIP proposal to support the inclusion of these changes in a future Zcash network upgrade.
    iv. Supporting the ZIP proposal through the inclusion process and helping to ensure its successful implementation.
    v. Developing a reference implementation of a secure messaging application built on top of the extended memo field.

Project tasks:

a. Stage 1: ZIP Proposal:
    i. Develop a detailed design document outlining the proposed extension of the memo field and the reference implementation of the secure messaging application.
    ii. Conduct a thorough security and performance analysis of the extended memo field design.
    iii. Develop a ZIP proposal for the extension of the memo field and its inclusion in a future Zcash network upgrade.
    iv. Engage the Zcash community to establish consensus on whether or not to implement the proposal.
b. Stage 2: Implementation
    i. Implement the extended memo field and the reference implementation of the secure messaging application.
    ii. Conduct a thorough security analysis of the reference implementation of the extended memo field.
    iii. Provide user documentation for the reference implementation.

Project deliverables:

- The contractor(s) will be required to deliver:

i. A detailed design document outlining the proposed extension of the memo field and the reference implementation of the secure messaging application.
ii. Security and performance analysis of the extended memo field design.
iii. A ZIP proposal for the extension of the memo field and its inclusion in a future Zcash network upgrade.
iv. Implementation of the extended memo field and the reference implementation of the secure messaging application.
v. Security and performance analysis of the extended memo field reference implementation.
vi. User documentation for the reference implementation.

## 4. Proposal Requirements

The Proposal shall outline the Grantee's Scope of Services, which at minimum must include the criteria set forth within this Request for Proposal, and the Grantee's approach to administer and complete the project.

A detailed project approach will assist ZCG in understanding the Grantee's comprehension of the project and the opportunities and constraints that a project of this complexity may contain. At a minimum the Proposal shall include the following:

- Cover letter detailing what specifically qualifies them to execute the project (maximum 1 page)
- Project approach including any details on the design approach and clearly identify all assumptions such as estimated increase to transaction size and client performance cost (appropriate length for the complexity of the specific project)
- Project process (check-ins, sign-offs, other applicable process actions)
- Project team organizational chart
- Response to Section 10, if applicable
- Resumes (2 page maximum per resume) for key project personnel and any subcontractors to be used (unless prohibited by a specific SOW)
- Samples of applicable work (attachments or links)
- Itemized budget with any milestone payments clearly tied to completed intermediate deliverables
- Any supplementary materials relevant to the project

## 5. Additional Comments

Extending the Zcash memo field will require changes in the consensus mechanisms within zcashd and zebrad. Ideally we would like to receive proposals for which the applicant is able and willing to contribute code to these code bases. However, we will also accept proposals from applicants who can design and deliver the ZIP proposal and a separate

reference implementation with the expectation that ECC/ZF may implement the ZIP in zcashd/zebrad themselves.