

xxRFP-2022-004

xxQuery: Anonymous Querying to Non-Anonymous Services

This xx foundation request for proposals will fund the creation of xxQuery, a tool that facilitates anonymous querying and reception from non-anonymous services. For example, a user can use this tool to search for an article on Wikipedia or query Wolfram Alpha while concealing their identity. This tool is similar to accessing a website via a proxy or onion routing; however, it provides better privacy and anonymity by sending the query over cMix and interfacing directly with services to avoid possible tracking or identification via fingerprinting.

The xx foundation is offering a competitive bidding process to complete this work, with independently compensated phases. The [selection process](#) will analyze each phase individually according to the response contents, the proposed compensation, and the proposed final deliverable dates and contents. Proposers are expected to propose for all phases.

Requirements

xxQuery should provide a UI to allow users to submit a string to a service and receive a response. For example, a user can submit a search term to a wiki and receive an article in response.

All requests from the users and responses from the service pass through a server on the xx network, limiting those services' ability to know the owner of the request.

Proposals should discuss methods to integrate with services in such a way as to limit metadata exposure and prevent blocking due to anti-spam measures.

Proposals can focus on integration with a single service or a group of services.

Architecture

A cMix client running as a server will receive requests from users, connect with the service, and transmit the response back to the server, which then sends it back to the user. A user's request remains encrypted and anonymous when transmitted to the server over cMix. However, once the server communicates with the external service, any contents in the request or the response cannot be guaranteed to be encrypted. Although, when possible, available encryption schemes, such as TLS, should be used.

To retain the user's anonymity and privacy on the xx network, two possible protocols can be used: [single-use messaging](#) or creating a new ID and using [connections](#). The [REST-like](#) API utilizes both these protocols and can be used to facilitate querying services.

Single-use allows a simple request and response but is bandwidth limited and once the response has been received, the connection is terminated. This may be appropriate for one-off, low-bandwidth usage.

However, high-bandwidth requests or responses will require generating a new ID and using connections to communicate small messages and [file transfer](#) to handle large messages. For example, sending a request for an image.

Phases

You may propose your own phases, but the following phases are desired:

Phase 1: Proof of Concept—Implement the basic version of your proposed design and submit a final design for the client-side and server-side functionalities. This should include final versions of any cryptographic primitives and fully explained versions of all data structures and sub-protocols, as well as discussions on integration with a service.

Phase 2: Software

- **Server-Side Software**—Build a server client that can anonymously query and receive a response from an external service.
- **Command-Line Tools**—Fully functional client-side command-line tool which fully exercises your proposed system without a user interface. The client-side command-line tool is the final library used by the Android and iOS apps, with test coverage of at least 85% of the code base and an accompanying continuous integration/continuous deployment (CI/CD) styled testing script.

Phase 3: User Facing App

- **Android App**—Android app with the final user interface design using the library from Phase 2.
- **iOS App**—iOS app with the final user interface design using the library from Phase 2.

Submission Instructions

Proposers should submit their proposals, in English, to the following website:

- <https://xxfoundation.org/archive/xx-foundation-announces-the-xx-dapps-grant-program>

Note that proposals are divided into two parts: An anonymized technical proposal and a staffing proposal. The technical proposal will be posted online and should not contain any identifying information about your organization or staff. The staffing proposal will contain resumes and additional evidence for why you and your team are qualified to do the work you propose.