# Zecwallet Lite Client
# Security Audit Proposal
# Concision Systems


## Scope

Concision Systems has requested that Least Authority perform a security audit of the Zecwallet Lite Client, a Rust library and Command Line Interface (CLI) that utilizes ZecWallet light client protocol to maintain and run a wallet.

## Code

The following code repositories are considered in-scope for the review:

- Zecwallet Lite Client: https://github.com/adityapk00/zecwallet-light-cli/

However, the following repositories, in addition to any dependency and third party code, are considered out of scope:

- Server: https://github.com/adityapk00/lightwalletd
- Electron Desktop Application: https://github.com/adityapk00/zecwallet-lite/
- iOS and Android Applications: https://github.com/zecwalletco/zecwallet-mobile

## Documentation

The following documentation is available to the review team:

- Light Client Protocol for Payment Detection: https://zips.z.cash/zip-0307
- README: https://github.com/adityapk00/zecwallet-light-cli/blob/master/README.md
- Commands documentation: https://github.com/adityapk00/zecwallet-light-cli/blob/master/lib/src/commands.rs

## Areas of Concern

The following are areas of concern that will be investigated during the audit, along with any similar potential issues:

- Correctness of the implementation and its adherence to the protocol specification;
- Common and case-specific implementation errors;
- Vulnerabilities in the wallet code, as well as secure interaction between the related and network components;
- Key management: secure private key storage and proper management of encryption and signing keys;
- Attacks that impacts funds, such as the draining or the manipulation of funds;
- Mismanagement of funds via transactions;
- Adversarial actions and protection against malicious attacks;
- Inappropriate permissions and excess authority;

- Data privacy, data leaking, and information integrity; and
- Anything else as identified during the initial analysis phase.

## Schedule

The following schedule is planned:

- **January 25 - February 9**: Code review completed
- **February 11**: Delivery of Initial Audit Report
- **TBD:** Verification completed
- **TBD:** Delivery of Final Audit Report

The above dates are based on our availability at the time this proposal was created and are not to be considered confirmed until an agreement to perform the proposed work is signed. The schedule is also subject to change based on team availability and readiness of the project for audit. If both teams agree that certain areas of concern should receive additional attention, the project schedule may be modified or extended.

The dates for verification and delivery of the Final Audit Report are subject to change and will be determined upon notification from our client that the code is ready for verification.

## Project Phases

Least Authority will investigate the areas of concern and assist with resolving any issues discovered during the audit with the following phases.

#### Review Phase

- **Project Discovery and Planning:** We would like to start this project with a kick-off meeting to get an overview of the service from the perspective of the client and the technical leads. We will also discuss what resources need to be shared, revisit the project schedule and agree upon necessary communication channels.
- **Exploration and Implementation Investigation:** In this phase we read design documentation, review other audit results or resources, and generally prepare for where vulnerabilities may be present. We will log our efforts to find vulnerabilities and related potential issues. Throughout the project we will hold meetings and share notes as is appropriate, depending on the process and focus of the investigations. We will also capture notes on how any issues that we do find could be mitigated or resolved.
- **Initial Audit Report Delivery:** At this point in our schedule, we wrap up our investigative work, document any unresolved issues or open questions and suggested resolutions in the report. This report is intended for internal use, only. A meeting to discuss the results of the report is recommended.

#### Resolution and Verification Phase

- **Remediation:** After delivering the report, we will be available for consultation, as needed. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.
- **Verification:** When the development team believes that all issues with sufficient impact have been addressed, we will review the system to confirm that these changes are made. It may be the case that some resolutions need to be discussed further because of the nature of design, code, operational deployment, and other engineering changes, as well as mistakes or misunderstandings.

- **Updated Audit Report Delivery:** We will update our report to reflect the resolved or mitigated status of any issues in the initial report. We will collaborate with the developers to make sure we all can agree that the report is appropriate to share publicly, but still transparent about and true to our original findings. Only after we agree with the development team that all vulnerabilities with sufficient impact have been appropriately mitigated do we publish our results.

## Deliverables

An Initial Audit Report will be provided after the initial review and a Final Audit Report will be provided at the conclusion of verification phase of the project. Throughout the project we will hold meetings and share notes as is appropriate, depending on the process and focus of the investigations. These deliverables could also include code suggestions, instructions, or other forms of supporting material.

## Publication & Responsible Disclosure

After verification is completed and the Final Audit Report is delivered, public release of the report is optional. The process for publication usually includes a post on the Least Authority website, however, all parties to the agreement will have an opportunity to discuss and agree upon details prior to publication.

Least Authority is committed to its clients and will work to ensure our clients have the appropriate information and time needed to address threats and vulnerabilities identified during our initial audit. In an effort to stay true to our mission of promoting ethical practices as it relates to security and privacy, Least Authority also has a responsibility to the developers, users, and broader community utilizing the tools and technologies which we audit. For this reason, Least Authority tries to adhere to the principle of responsible disclosure, followed by full disclosure as a last resort. In support of this effort, we permit our clients' development teams the opportunity to address any issues prior to publicly disclosing our findings. In the event that our client is a third party, neither the development team nor related to the team responsible for addressing the issues found during the audit, we reserve the option to disclose any issues to the development team to allow them the opportunity to sufficiently address and respond to the issues prior to sharing our findings with the third party client. In the event that issues are not addressed by the development team in a timely manner and users are at risk, this will result in a public disclosure of our findings.

## Budgets

Total Cost for code review, reporting, remediation and mitigation support and verification: **48,038.00€** (not including VAT, if applicable). A 10% Community Funding Discount has been applied.

- 14,412.00€ will be invoiced upon signature of the agreement
- 28,366.00€ will be invoiced at the completion of the Initial Audit Report
- 5,260.00€ will be invoiced at the delivery of the Final Audit Report after the verification has been completed.

The above budgets are Fixed Price and not based solely on or limited to a specific number of person-days. We take this approach in order to adequately cover the audit scope and may assign additional team members as needed during the course of the audit. We find that the quality of our work is benefited by having several team members with a diverse set of skills conducting any given review.

# Project Team

Least Authority approaches review projects from a holistic perspective. To effectively cover the requirements for each project, we have several different team members participate in a review in order to best utilize their various specialized skill sets. The Least Authority team has skills for reviewing code in C, C++, Python, Haskell, Rust, Node.js, Solidity, Go, Java, JavaScript, TypeScript, C#, Swift, Kotlin, OCaml, Michelson, LIGO and SmartPy for common security vulnerabilities and specific attack vectors.

The following team members are proposed for this review:

**Bryan Chris White, Security Researcher and Engineer**
Bryan has spent over a decade in software engineering / programming, while living in 4 countries across 3 continents. A maker / hacker in his spare time, Bryan likes to automate and improve every-day processes and experiences. In addition to being a core contributor to storj.io / tardigrade.io, his skills include systems and network engineering. Passionate about free and open software, autonomy, and privacy, Bryan is always eager to learn new things.

**Dominic Tarr, Security Researcher and Engineer**
Dominic has been using node.js since version 0.2.1 and has published hundreds of open source javascript modules, known for his work in streams, databases, and database replication this lead to an interest in cryptography and security and developing the secure-scuttlebutt protocol.

**Dylan Lott, Security Researcher and Engineer**
Dylan is a distributed systems engineer specializing in peer-to-peer networks. He previously worked at Storj building their DHT and overlay network. He works mostly in Go, JavaScript, and Python. He's working on a database in his spare time and lives in Salt Lake City, Utah.

**Hind Kurhan, Senior Program Manager**
Hind began her work in software design project / program management after studying politics and economics. She eventually decided to pursue a career in human rights, humanitarian, and development work which would bring her back to Europe, the Middle East, and Africa - where she grew up. Her passion for human rights (including privacy, security, and freedom of speech) and her experience in management in the “tech” world lead Hind to pursuing opportunities in the data privacy and security world.

**Jan Winkelmann, Security Researcher and Engineer**
Jan is a software engineer primarily working in Go. His interests lie in the intersection of systems design, security and cryptography. He is currently working on secure scuttlebutt to advance the state of secure decentralized tools for collaboration.

**Jessie France, Project Manager**
Jessie joined Least Authority as a project manager and focuses her efforts on supporting security consulting projects and the operations infrastructure. She has a background in project, operation, and resource management in a variety of sectors.

**Liz Steininger, CEO / Managing Director**
Liz is a supporter of open source software that encourages transparency and access to information, along with software that enables individuals to freely express themselves and retain the ability to control their own information. She has over 17 years of experience as a Program and Project Manager, Strategist and Analyst working towards these goals.

**Mirco Richter, Cryptography Researcher and Engineer**

Mirco is a mathematician and computer scientist living in Berlin. He has been working and conducting research in the Blockchain space since 2011 and mostly focuses on Cryptography and Consensus Algorithms.

**Mohamed Jehad Baeth, Security Researcher and Engineer**
Jehad is an academic and a software engineer who enjoys solving complex problems and has an unrelenting dedication to learning new things in the rapidly evolving tech field. Beside working in a few reputable software companies, he has a research interest focusing on misinformation propagation in social networks and online privacy. Jehad has a PhD from Yildiz Technical University. He is currently contributing to various security audit projects.

**Nathan Ginnever, Security Researcher and Engineer**
Nathan is the founder of Finality Labs and is an applied cryptographer well versed in distributed systems, including blockchain protocols. He has extensive knowledge in smart contracts and has contributed to Ethereum state channel and other layer 2 designs. Nathan has written GPU parallel programming for ZCash and Filecoin and has contributed to open source projects like IPFS.

**Ramakrishnan Muthukrishnan, Security Researcher and Engineer**
Ramakrishnan (Ramki) is a computer programmer and lives in Bangalore, India. In the past, he has contributed to a bunch of Free software projects like the Debian project, GNU Emacs, Linux kernel and the GNU Radio. He likes to tinker with low-level system software and also enjoys learning and playing with Functional Programming. In his free time, he likes to play with electronics and amateur radio.

## About Least Authority

We believe that people have a fundamental right to privacy and that the use of secure solutions enables people to more freely use the Internet and other connected technologies. We provide security consulting services to help others make their solutions more resistant to unauthorized access to data and unintended manipulation of the system. We support teams from the design phase through the production launch and after.

The Least Authority team has skills for reviewing code in C, C++, Python, Haskell, Rust, Node.js, Solidity, Go, and JavaScript for common security vulnerabilities and specific attack vectors. The team has reviewed implementations of cryptographic protocols and distributed system architecture, including in cryptocurrency, blockchains, payments, and smart contracts. Additionally, the team can utilize various tools to scan code and networks and build custom tools as necessary.

To see a list of our published audit reports: https://leastauthority.com/blog/all-published-audits/.

Least Authority was formed in 2011 to create and further empower freedom-compatible technologies. We moved the company to Berlin in 2016 and continue to expand our efforts. Although we are a small team, we believe that we can have a significant impact on the world by being transparent and open about the work we do.

For more information about our security consulting, please visit https://leastauthority.com/security-consulting/.