Fine penetration tests for fine websites

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Audit-Report Project 11 Crypto Web UI & Backend 06.2025

Cure53, Dr.-Ing. M. Heiderich, Dr. N. Kobeissi

Index

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Introduction

This report, identifiable as P11-01, presents the outcomes of a cryptography review and source code audit against the Project 11 yellowpages client and backend, as performed by Cure53 in early June 2025.

For background information, representatives from Project 11 Limited contacted Cure53 in May 2025 to request the assessment and specify the overall aims. The initiatives were completed over a one-week period (CW23) by a two person review team. Four days were allocated for the analysis, which was deemed an ample time frame to achieve the expected coverage and yield of results.

Two individual Work Packages (WPs) were created for the examinations, denoting the key areas of interest. These read as follows:

- **WP1**: Cryptography reviews & source code audits against Project 11 FE crypto
- **WP2**: Cryptography reviews & source code audits against Project 11 BE crypto

Cure53 received source code, a whitepaper, and all other necessary means of access to conduct the tests and reviews, employing a white-box methodology. All preparations were completed in late May 2025 (CW22) to ensure a seamless start.

Communication throughout the assignment occurred via a dedicated Slack channel, which included all relevant personnel from both Project 11 and Cure53. The cross-team discourse was generally seamless, with minimal need for clarification as the scope was clearly defined and well-prepared. No significant obstacles arose during the testing period.

Cure53 provided regular status updates on the progress and identified findings. Live reporting was also offered and deemed beneficial for this exercise, conducted via the designated Slack channel.

Following satisfactory depth and breadth of coverage over the scope elements, Cure53 detected and documented a total of four findings in ticket format. One was classified as security vulnerability, while the remaining three were filed as miscellaneous weaknesses.

This audit of the Project 11 yellowpages client confirms that a technically competent approach to addressing the quantum threat to Bitcoin has been adopted. While the core cryptographic operations, TEE integration, and post-quantum algorithm implementations are sound, a fundamental tension exists due to the chosen centralized architecture, which introduces significant new centralization risks. Moreover, Cure53 observed areas for enhanced cryptographic engineering rigor, such as ineffective memory zeroing and a lack of formal analysis for cross-signature construction.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Despite these architectural and strategic concerns, solid baseline security practices are adhered to. Prior to production deployment, a fundamental re-evaluation of the aforementioned architecture is necessary, exploring alternative, trust-distributing approaches that align with Bitcoin's ethos.

The report will now provide insights into the *Scope* and testing setup, as well as display a comprehensive breakdown of all available materials in bullet point form. Subsequently, the report will list all findings identified in chronological order, starting with the *Identified Vulnerabilities* and followed by the *Miscellaneous Issues*. Each finding will be accompanied by a technical description and Proof of Concepts (PoCs) where applicable, plus any relevant mitigatory or preventative advice to action.

In summation, the report will finalize with a conclusion in which the Cure53 team will appraise the general security posture of the elements in focus, offering high-level hardening advice and next steps for the internal team.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Scope

- **Cryptography reviews & audits against Project 11 Crypto web frontend & backend**
  - **WP1:** Cryptography reviews & source code audits against Project 11 FE crypto
    - **Source code**:
      - **URL**:
        - https://github.com/p-11/yellowpages-client
      - **Branch**:
        - *development*
      - **Commit**:
        - *d0191650d61778119cc018c6b554e9dffd3adce9*
  - **WP2:** Cryptography reviews & source code audits against Project 11 BE crypto
    - **Source code**:
      - **URL**:
        - https://github.com/p-11/pq-address-ts
      - **Branch**:
        - *main*
      - **Commit**:
        - *e287760ce4b01e42dca2333d49319c441a548854*
      - **URL**:
        - https://github.com/p-11/pq-address-rs
      - **Branch**:
        - *main*
      - **Commit:**
        - *8f180b14523d777d52c0f95d6765307d3f76ea0b*
      - **URL**:
        - https://github.com/p-11/yellowpages-proof-service
      - **Branch**:
        - development
      - **Commit**:
        - *81fdb0ac6ceac0b213856516ea1a8bcba6cb866f*
      - **URL**:
        - https://github.com/p-11/yellowpages-verification-service
      - **Branch**:
        - development
      - **Commit**:
        - *79302565a9f95f5b28a08f68047a6ca5d4645e37*

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

- **Scope considerations & priorities:**
  - Functional correctness of utilized designs, implementations and algorithms
  - Attacks on features using methods described by current academic research
  - Possible timing attacks targeting algorithmic resistance
  - Constant-time operations & random number generation
  - Side-channels, information leaks, secure storage, and data processing
  - DoS vectors, information leakage, and logic bugs
  - Secure random number usage and generation
  - Secure handling of numeric values and floating point numbers
  - Existing third-party integrations & dependencies
  - Issues with wallet software and similar tools
- **Test-supporting material was shared with Cure53**
- **All relevant sources were shared with Cure53**

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Identified Vulnerabilities

The following section lists all vulnerabilities and implementation issues identified during the testing period. Notably, findings are cited in chronological order rather than by degree of impact, with the severity rank offered in brackets following the title heading for each vulnerability. Furthermore, all tickets are given a unique identifier (e.g., *P11-01-001*) to facilitate any future follow-up correspondence.

P11-01-002 WP2: Trusted Proving Engine creates single point of failure *(High)*

Client Note: *Project 11 appreciates the feedback regarding the Proving Engine as a potential single point of failure, as well as the broader concerns around the use of Trusted Execution Environments (TEEs) in Yellowpages. While we recognize that centralized components introduce risk, we do not believe this constitutes a present, high-severity Identified Vulnerability based on our threat model and current implementation.*

Project 11's response to each of the proposed issues about centralized TEE usage:

- ***Malicious Engine Scenario:*** *Users can independently verify proofs via downloaded PCR measurements, ensuring the output came from a valid TEE. Both client and proof-verification code will be open-sourced next week, making it possible to detect any malicious behavior immediately.*
- ***Quantum Compromise:*** *The suggested scenario of a future quantum attack assumes a successful breach of the Nitro Enclave, which currently has no known practical vulnerabilities. Moreover, the enclave does not persistently store Bitcoin public keys, limiting potential exposure even in the event of compromise.*
- ***Correlation Attacks:*** *Our public documentation advises users not to share their proofs if they wish to preserve anonymity. We do not collect identity metadata or IP addresses, so correlation from our side is not possible.*
- ***TEE Security Practices:*** *We monitor Nitro-related CVEs and coordinate with our TEE provider (Evervault) to apply patches as they are released, consistent with standard practices for hardware-backed systems.*

In conclusion, there are no known exploitable defects at this time. While we plan to explore alternatives like ZK in future versions, the current trade-offs around maturity and quantum resistance led us to opt for a TEE-based design in v1. We will ensure that trust assumptions and TEE usage are clearly documented across the whitepaper, guides, and public materials.

Cure53's review of the yellowpages cryptographic design revealed that the system utilizes encrypted channels and TEE attestation. However, the implementation still relies on a centralized Proving Engine that receives Bitcoin public keys and creates centralized proof records, which induces significant privacy and centralization risks.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

An attacker that is able to compromise the Proving Engine can collect Bitcoin public keys for future quantum attacks, correlate user identities with Bitcoin addresses, and create a centralized database of quantum-vulnerable keys.

While immediate theft is implausible, the system creates a high-value target containing the exact information required by quantum attackers. Additionally, the reliance on AWS Nitro Enclaves introduces hardware vendor trust assumptions.

Furthermore, the web interface does not provide a means by which to independently verify its output. Users must rely on the web interface's provision of honest results, corresponding to the TEE-backed cryptographic implementation that yellowpages advertises.

A number of attack scenarios are viable in this context, including:

- **Malicious Proving Engine:** The Proving Engine is currently accessible via a centralized web interface, through which queries for which *Bitcoin addresses are post-quantum secure*[1] are issued. A web of trust has not been established, while the web interface is not restricted from issuing misleading results to querying users. Project 11 has removed the above wording from the website during the course of the audit.
- **Future quantum compromise:** An adversary could compromise the Proving Engine, harvest all registered Bitcoin public keys, and simply wait for quantum computers to break them.
- **Privacy correlation:** Timing analysis of proof submissions could link user identities to Bitcoin addresses.
- **TEE compromise:** Vulnerabilities in AWS/Intel hardware could expose the attestation process.

The centralized proving engine creates an inherent trust requirement that largely contradicts modern cryptographic best practices, where state-of-the-art privacy systems increasingly adopt zero-knowledge proofs specifically to eliminate such single points of failure. Production-ready ZK implementations from projects like Aztec and Zilch demonstrate the maturity of this technology, with extensive research addressing post-quantum security concerns. Furthermore, the reliance on a web interface for most user interactions introduces standard web security limitations—including MITM attacks, DNS hijacking, and JavaScript trust assumptions—that TEE attestation cannot fully address.

[1] The yellowpages service asks users to "Enter a Bitcoin address to check if it's post-quantum secure." This statement is highly misleading, since the yellowpages service cannot guarantee Bitcoin address post-quantum security. At best, it can only check if a Bitcoin address is signed with an ML-DSA and SLH-DSA key pair, while verifying that the Bitcoin address itself signed the ML-DSA and SLH-DSA key pairs at an earlier point in time.
Project 11 removed the quoted statement from the yellowpages website during the course of the audit.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

The High severity classification reflects the systemic impact of this architectural decision on the platform's security model. While the client has implemented certain safeguards, the centralized trust requirement fundamentally limits the security guarantees the system can provide. Users must trust the proving engine during proof generation, regardless of post-facto verification capabilities.
This design choice represents a significant deviation from the decentralized, trustless architectures that define current best practices in privacy-preserving systems. The vulnerability classification considers not just immediate exploitability but also the constraint this architecture places on the system's ability to provide strong privacy guarantees without trusted intermediaries.

To mitigate this vulnerability, Cure53 advises redesigning yellowpages to ensure that users can obtain client-side, verifiable assurance of the correctness and honesty of both its computations and attestations on behalf of other Bitcoin public wallets.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Miscellaneous Issues

This section covers any and all noteworthy findings that did not incur an exploit but may assist an attacker in successfully achieving malicious objectives in the future. Most of these results are vulnerable code snippets that did not provide an easy method by which to be called. Conclusively, while a vulnerability is present, an exploit may not always be possible.

P11-01-001 WP1: Ineffective memory zeroing for cryptographic keys *(Info)*

Fix note: *This issue was addressed during the testing phase. Cure53 verified that warnings were added, clarifying that the memory zeroing attempts were strictly "best effort". Project 11 clarified and demonstrated that they were aware that the approach was "best-effort".*

Testing confirmed that the *destroyMlKem768Keypair* function attempts to clear cryptographic material from memory using JavaScript's *fill()* method. However, this approach is insufficient for secure memory clearing in JavaScript environments, due to potential compiler optimizations and garbage collection behavior.

This circumstance allows sensitive cryptographic key material to persist in memory for extended durations, potentially enabling memory dump attacks or forensic recovery of the ML-KEM-768 keypair data. While the attack surface is limited to local memory access, the exposure of post-quantum cryptographic keys could compromise the secure channel establishment. JavaScript engines may optimize away the zeroing operation if the memory is scheduled for garbage collection. Furthermore, key material may have been copied to other memory locations during garbage collection cycles.

Affected file:
yellowpages-client/src/core/cryptography.ts

Affected code:

```
function destroyMlKem768Keypair(keypair: MlKem768Keypair): void {
  // Zero out both keys
  keypair.encapsulationKey.fill(0);
  keypair.decapsulationKey.fill(0);
}
```

While an effective mitigation for this issue within the JavaScript ecosystem is not available at present, Cure53 recommends documenting the functionality as best-effort rather than retaining the current labeling, thus marking it as a definitive method of zeroing out keys from memory.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

P11-01-003 WP2: Cross-signature construction lacks formal security analysis *(Info)*

Cure53's review of the yellowpages design revealed that the proposed cross-signature scheme combining ECC and post-quantum signatures (ML-DSA and SLH-DSA) has not undergone formal security analysis or provable security verification.

This situation allows for potential cryptographic vulnerabilities whereby the combined scheme could be weaker than either constituent algorithm individually. Unexpected interactions between ECC and PQ signature schemes could introduce novel attack vectors that are not present in either system alone.

To mitigate this issue, Cure53 advises conducting formal cryptographic analysis of the cross-signature construction, including security proofs under standard cryptographic assumptions. Academic cryptographers could be consulted to verify the security properties of combining these signature schemes prior to production deployment.

P11-01-004 WP2: Governance lacks consensus/adoption mechanisms *(Info)*

The yellowpages design lacks clear mechanisms for achieving Bitcoin community consensus, preventing competing systems, and ensuring coordinated adoption across wallet providers and exchanges.

As such, ecosystem fragmentation could occur whereby multiple competing yellowpages systems emerge, reducing security via user confusion and diluted adoption. The absence of standardized integration pathways could prevent widespread adoption when quantum threats materialize.

To mitigate this issue, Cure53 recommends developing a governance framework involving key Bitcoin stakeholders, establishing technical standards via Bitcoin Improvement Proposals (BIPs), and creating reference implementations for wallet integration to ensure ecosystem-wide compatibility.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Conclusions

This Q2 2025 security engagement focusing on yellowpages revealed a technically competent implementation that attempts to solve one of Bitcoin's most existential challenges, the quantum threat. The core cryptographic operations are integrated correctly, the TEE integration follows best practices, and the post-quantum algorithms are adequately installed. However, the findings reveal a fundamental tension between the desire to provide quantum protection and the architectural decisions that introduce new centralization threats. For instance, P11-01-002 highlights that the centralized yellowpages architecture risks trading one threat for another via a centralized verification interface that is difficult to independently verify for correctness and honesty.

The Project 11 team demonstrates astute understanding of post-quantum cryptography implementation standards. The ML-KEM-768 key exchange, signature verification logic, and TEE integration all conform to established patterns.

However, P11-01-003 may hint at a deviation from long-established cryptographic engineering best practices. The lack of formal analysis for the cross-signature construction indicates that the internal team may be unaware of the complexities involved in combining cryptographic primitives. While we stress that this discovery should not be considered a fundamental flaw, it may indicate that the cryptographic engineering requires additional hardening before production deployment.

P11-01-004 exposes a significant strategic weakness, whereby the Project 11 team has focused intensely on the technical implementation, while seemingly overlooking the equally critical challenge of ecosystem adoption. Bitcoin's notoriously conservative governance makes coordinated upgrades extremely difficult, yet yellowpages lacks clear mechanisms for achieving community consensus or preventing ecosystem fragmentation. This is pertinent from a security perspective, since it could eventually allow for ecosystem fragmentation where multiple competing yellowpages systems emerge, reducing security through user confusion and diluted adoption. The absence of standardized integration pathways could prevent widespread adoption when quantum threats become practicable.

The yellowpages codebase was generally well-prepared for this security evaluation, with clear documentation and accessible source code. The in-house team was responsive during testing and demonstrated genuine security awareness.

In summary, the pitfalls outlined in this report represent a comprehensive overview of the system's security posture, from low-level implementation details to high-level architectural concerns. Notably, no *Critical* exploitable vulnerabilities were located in the core implementation, suggesting that the development team conforms to contemporary security practices.

Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

The yellowpages client faces a classic security trade-off dilemma, in the sense that the proposed cure introduces new risks that may be worse than the disease. The centralized architecture that enables practical deployment also creates the systemic hazards that Bitcoin was designed to avoid. Before pursuing production deployment, the maintainers should fundamentally reconsider whether centralized quantum protection can ever be compatible with Bitcoin's trustless principles.

Alternative approaches worth exploring include decentralized proof systems, gradual protocol-level upgrades, or hybrid models that distribute trust across multiple independent operators. The technical execution quality suggests that the handlers are capable of building their architecture of choice. The critical decision is selecting an architecture that Bitcoin users would actually trust and adopt.

Cure53 would like to thank Conor Deegan and David Nugent from the Project 11 Limited team for their excellent project coordination, support, and assistance, both before and during this assignment.