Security assessments for software that matters.

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

Pentest-Report Worldcoin Attestation Gateway Repository 11.2025-01.2026

Cure53, Dr.-Ing. M. Heiderich, MSc. J. Moritz, M. Pedhapati, M. Piechota

Introduction

> *"World App is a super app for humans in the age of AI. It features the first wallet created for World and gives people access to a private, decentralized proof of human through World ID and access to decentralized finance through cryptocurrencies."*
>
> From https://world.org/faqs

This report details the findings of a source code audit and penetration test conducted on the Worldcoin Attestation Gateway library. While this library represents a specific aspect within the broader World and Orb application complex audit, this standalone document was requested to provide a dedicated overview of its security posture.

The assessment was executed by Cure53 between November 2025 and January 2026, following the initial request from Tools for Humanity Corp. in October 2025. The engagement was scheduled to account for the significant scale and multi-component nature of the architecture. This task marks the second collaboration between the two organizations, building upon the insights gained from the previous TFH-01 inspection.

In terms of the exact timeline and specific resources allocated to TFH-02, the Cure53 analysts completed their research across two separate periods spanning several months, namely in November and December 2025 (CW47 to CW49) and January 2026 (CW02 to CW04).

In order to achieve the expected coverage of the targeted attributes, a total of seventy-four days were invested. A team consisting of sixteen senior testers was formed and assigned to the task's preparation, execution, documentation, and delivery.

While the scope of TFH-02 was divided into seven distinct Work Packages (WPs), only a single variant was relevant for this report, entitled *WP2: White-box penetration tests & code audits against World app backend & API*.

A white-box testing strategy was adopted, supported by the provision of all relevant source code and test credentials. Cure53 received the full suite of access required to complete the investigations, ensuring alignment with the wider objectives. This approach allowed for a highly detailed examination of the application's codebase and corresponding execution paths.

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

The consulting team's efforts proceeded according to plan, remaining free of major technical or administrative setbacks. To ensure a high level of operational efficiency, all preliminary preparations were finalized in mid-November 2025 (CW46). These early measures allowed the Cure53 team to transition smoothly into the active analysis phase without delay.

For transparent communications, a dedicated Slack channel was established as the primary collaborative hub. This shared environment allowed the Cure53 and Tools for Humanity stakeholders to participate in direct dialogue. This method proved vital for verifying findings and ensuring that all participants remained informed of the general progress.

Minimal clarification questions were required and the project-related interactions were seamless. The testing team provided frequent status updates to keep the internal maintainers in the loop. Given the project's extended duration, live-reporting was utilized to ensure that emerging discoveries were relayed immediately, allowing for a proactive response to vulnerabilities. The shared Slack channel was central to this agile approach, allowing selected findings to be reported to the Tools for Humanity team while examinations were still underway.

This continuous communication significantly enhanced the project's overall efficacy. Furthermore, no significant roadblocks were encountered, a success attributed to both the meticulous initial scoping and the ongoing support provided by the development team.

Regarding the specific results for the Attestation Gateway library, the Cure53 team achieved comprehensive testing coverage but identified no vulnerabilities or findings. This outcome is a highly positive indicator of the library's current security posture, demonstrating that the existing defensive measures and code quality are sufficiently robust to withstand rigorous white-box scrutiny.

While these results are promising, it is important to reiterate that the Attestation Gateway library was audited as one component within a substantially sized ecosystem. To attain granular understanding of its resilience, a standalone initiative focusing exclusively on this library may be beneficial. Nevertheless, the absence of exploitable flaws during this round attests to first-rate security integrity.

The following sections first describe the scope and key test parameters, as well as the structure and organization of the work packages. Next, all findings are presented in ticket format. The problems are discussed chronologically within each category. In addition to technical descriptions, PoCs and mitigation advice are provided where applicable.

Lastly, the report culminates with general conclusions relevant to this late 2025 to early 2026 project. Based on the test team's observations and the evidence collected, Cure53 elaborates on the overall impressions and reiterates the final verdict. This section also includes tailored hardening recommendations for the World app Attestation Gateway library.

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

Scope

- **Penetration tests & code audits against World app Attestation Gateway library**
  - **WP2:** White-box penetration tests & code audits against World app backend & API
    - **Attestation gateway source code:**
      - URL:
        - https://github.com/worldcoin/attestation-gateway
      - Commit:
        - a95d4acfa083d82e278552eb483da3aeaa35bbb8
  - **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

Test Methodology

This section documents the testing methodology applied by Cure53 during this project and discusses the resulting coverage, shedding light on how various components were examined. Further clarification concerning areas of investigation subjected to deep-dive assessment is offered, especially in the absence of significant security vulnerabilities detected.

The attestation-gateway is a Rust-based backend service that acts as an integrity verification layer between mobile clients and downstream services. The service receives platform-level attestation proofs from Android Google Play Integrity and iOS Apple DeviceCheck, verifies them locally, and issues signed JWTs. Downstream services utilize these to confirm that requests originate from legitimate, untampered application instances running on genuine devices.

The attestation gateway offers two main routes. Firstly, */g* is the core token generation endpoint that receives an attestation request containing a platform-specific integrity proof, bundle identifier, and request hash from the mobile client. The requestHash is generated on the client side by Oxide's AttestRequestHash module within the World App.

Based on the bundle identifier, the request is routed to the appropriate verification path, Android Play Integrity, and Apple DeviceCheck. If the proof passes all validation checks, the service signs and returns a JWT attestation token via AWS KMS.

For the downstream service, */.well-known/jwks.json* serves the JSON Web Key Set containing the public keys employed for attestation token signing. These services call the endpoint to verify the token issued by the */g* endpoint.

All signing operations are handled exclusively by AWS KMS using ES256. The private key material is never loaded into application memory at any point in the token lifecycle.

The key rotation mechanism was systematically reviewed and deemed correctly implemented. The function employs a 180-day signing TTL and 182-day verification TTL. Cure53 did not locate any issues related to key management or cryptographic misuse during the engagement.

For Android, the Play Integrity verification follows a five-step validation process: package name validation, nonce binding, timestamp freshness checks, certificate SHA-256 digest comparison, and device integrity verdict verification. Similarly, the testers did not detect any erroneous behaviors in this area.

Lastly, replay attack prevention is astutely enforced via Redis for request hash deduplication. The Apple DeviceCheck implementation adheres to Apple’s specification, including the nine-step initial attestation verification and five-step assertion counterpart. This aspect was also deemed risk averse.

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

Conclusions

The *Conclusions* section offers a deeper analysis of the research scope, validated findings, and the final architectural verdict. In summary, Cure53 can confirm that the inspections produced favorable results, as reflected by the complete absence of security threats to report.

The Worldcoin Attestation Gateway scope is a feature of the broader World App backend and API, which handles the Android Play Integrity and Apple DeviceCheck to ensure that World App operates on a legitimate, untampered device prior to allowing backend service communication.

The service was subjected to a thorough white-box source code evaluation, focusing on three primary routes: the token generation endpoint (*/g*), the JWKS public key endpoint (*/.well-known/jwks.json*), and the underlying cryptographic verification logic for Android Play Integrity and Apple DeviceCheck. Regarding the cryptographic premise, the analysis determined that all signing operations are delegated exclusively to AWS KMS using ES256. Private key material never exists in application memory at any stage during the token lifecycle.

The key rotation logic leverages a 180-day signing TTL and a 182-day verification TTL. This element was diligently inspected and confirmed to be appropriately implemented. Malpractices related to key management and cryptographic abuse are successfully neutralized. Onward, Cure53 noted that the Android Play Integrity verification implements a five-step claim validation chain covering package name, nonce binding, timestamp freshness, certificate SHA-256 digest comparison, and device integrity verdicts. The auditors did not unearth any negative activities here.

The Apple DeviceCheck construct conforms to Apple's specification, inclusive of its nine-step initial attestation verification and five-step assertion verification. The codebase exhibits robust input validation and error segregation. Moreover, logging is enforced in a sound manner, minimizing the likelihood of information leakage.

To finalize, Cure53 is pleased to verify that the attestation-gateway offers a performant security posture and defense-in-depth architecture, with hardware-backed cryptographic operations that prioritize separation of trust boundaries. By delegating all signing to AWS KMS, the service establishes a foundation that mitigates sophisticated attestation forgery and replay attacks.

Cure53 would like to thank Vincent Junik, Juan Broullon, Christian Privitelli, Subhodeep Bose, Mikhail Khakhel, Denys Davydoy, Paolo D'Amico, Aleksandr Vygodchikov, Nicolas Vaquero, Murph Finnicum, Andrew Wang, and Panagiotis Kakalis from the Tools for Humanity Corp. team for their excellent project coordination, support, and assistance, both before and during this assignment.