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

Cure53 Security Assessment of IDZ Crypto Libraries, Mobile & Web, Management Summary, 09.2025

Cure53, Dr.-Ing. M. Heiderich, M. Wege, Dr. D. Bleichenbacher, J. Hector, Dr. M. Conde, Dr. N. Kobeissi

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a penetration test and source code audit performed against a wide array of IDZ applications, components, and associated cryptographic libraries, and architectures.

The engagement was commissioned by IDZ in July 2025 and carried out by Cure53 in September 2025 (CW39). Twenty-one days were dedicated to achieving the required coverage for this project.

The entire scope of work was divided into seven distinct Work Packages (WPs), detailed as follows:

- **WP1:** White-box code reviews & audits against IDZ key derivation architecture
- **WP2:** White-box code reviews & audits against IDZ zcrypto Dart library
- **WP3:** White-box code reviews & audits against IDZ client crypto C++ library
- **WP4:** White-box pen.-tests & Audits against IDZ backend key-management
- **WP5:** White-box pen.-tests & assessments against IDZ iOS & Android apps
- **WP6:** White-box pen.-tests & assessments against IDZ Flutter web apps
- **WP7:** White-box pen.-tests & assessments against IDZ backend APIs

Cure53 received the necessary provisions to conduct the evaluations, including source code, binaries, URLs, documentation, and test-user credentials, thereby utilising a white-box methodology. Six security analysts were assigned to conduct the initiative's preliminary arrangements, operational execution, and final conclusion.

To ensure a seamless commencement, all necessary preparatory work was finalized in September 2025 (CW38). A dedicated collaborative Slack channel was used to facilitate all interactions throughout the assessment, and all relevant personnel from both IDZ and Cure53 were invited.

The project’s meticulously defined and unambiguous parameters ensured that exchanges were seamless and required minimal clarification. No significant impediments were encountered during testing. Cure53 provided regular progress reports and findings, and utilized shared Markdown files to offer live-reporting for all High and Critical severity issues.

Achieving extensive coverage over the WP1-WP7 scope items, the Cure53 team identified a total of twenty findings. The discoveries were categorized as eleven security vulnerabilities and nine general weaknesses with reduced exploitation potential.

The audit confirmed a strong foundation in cryptographic primitives and secure usage of the backend Botan crypto library. Despite this, the review identified critical architectural and implementation flaws, including two Critical and six High-severity vulnerabilities. The IDZ team acted immediately to prioritize fixes, successfully resolving the majority of the most severe issues.

All Critical and High-severity issues have been successfully remediated and deployed by the IDZ team, apart from the Safety Number (Key Transparency) feature. The remaining paramount risk is the lack of authentication for long-term identity keys, which compromises the core End-to-End Encryption (E2EE) guarantee and is planned to be addressed in an upcoming release by the Safety Number (Key Transparency) feature. All lower ranking vulnerabilities have also been resolved, or otherwise mitigated. Yet, it is recommended by Cure53 to fully address all remaining issues and weaknesses in order to guarantee a safe and secure user experience.

Cure53 would like to thank Joseph Bara, Rohinton Collins, Dawid Fajkowski, and Michal Gruchota from the IDZ team for their excellent project coordination, support, and assistance, both before and during this assignment.