

Cure53 Security Assessment of Deeta Cryptographic Features, Management Summary, 09.2026

Cure53, Dr.-Ing. M. Heiderich, Dr. D. Bleichenbacher, Dr. S. Mazaheri

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a source code audit and review conducted against the Deeta cryptographic features and components.

To give some context regarding the assignment's origination and composition, Deeta LLC contacted Cure53 in August 2026. The test execution was scheduled for September 2026, namely in CW39. A total of six days were invested to reach the coverage expected for this project, and a team of three senior testers was assigned to its preparation, execution, and finalization.

The work was split into three separate work packages (WPs), defined as:

- **WP1:** Source-assisted reviews against Deeta share crypto & envelope format
- **WP2:** Source-assisted reviews against Deeta local key custody & Data-at-Rest
- **WP3:** Source-assisted reviews against Deeta plaintext & sync boundaries

To ensure maximum risk discovery and audit depth, the engagement utilized a white-box evaluation model. By granting total transparency into source repositories, system documentation, and environment access, Deeta enabled Cure53 to simulate highly informed threat actors and identify subtle, deeply embedded architectural vulnerabilities that surface-level testing would miss.

Thorough administrative setup concluded during CW38 of September 2026, creating an optimal foundation for project execution. Strategic coordination was driven through a shared Slack workspace containing all designated technical and leadership stakeholders from both organizations, ensuring seamless information exchange and organizational alignment throughout the testing lifecycle.

Engagement execution proceeded efficiently due to well-defined scope boundaries and complete pre-test preparation. Communication remained friction-free throughout the project, with minimal clarification required. Cure53 maintained continuous visibility through frequent status updates, real-time finding disclosures, and active live-reporting within the dedicated Slack workspace.

Assessment coverage across the agreed target surface was comprehensive, resulting in six identified security items. The overall risk distribution comprises three distinct security vulnerabilities requiring technical remediation and three broader architectural weaknesses representing lower immediate risk to business operations.

Identified Vulnerabilities

- DEE-01-002 WP3: Lack of forward-security in live profile syncing (Medium) **Fixed**
- DEE-01-003 WP1: Shared deets forwarding to unauthorized recipients (Medium) **Mitigated**
- DEE-01-005 WP1: Creating deets with arbitrary sender ID and name (Low) **Mitigated**

Miscellaneous Issues

- DEE-01-001 WP1: Incomplete key-separation (Info) **Fixed**
- DEE-01-004 WP1: One-sided contribution to share key (Info) **Intentional behavior**
- DEE-01-006 WP2: Rollback of pages encrypted with SQLCipher (Low) **Accepted risk**

The low overall volume of findings and the total absence of High or Critical severity vulnerabilities demonstrate a strong baseline security posture for the Deeta crypto features. These results confirm that foundational cryptographic logic and implementation patterns across the evaluated surface are resilient against severe technical exploitation.

Demonstrating strong engineering responsiveness, Deeta swiftly addressed all reported findings shortly following the active testing phase, successfully fixing or mitigating every identified vulnerability. The updated code fixes were provided directly to Cure53 and underwent formal re-testing, confirming full remediation across the entire assessment scope.

Cure53 would like to thank Peter Oram from the Deeta LLC team for his excellent project coordination, support and assistance, both before and during this assignment.