Security assessments for software that matters.

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

Cure53 Security Assessment of KIT KASTEL Enclave Flow & Config, Management Summary, 02.2026

Cure53, Dr.-Ing. M. Heiderich, Dr. A. Pirker, Dr. D. Bleichenbacher, MSc. D. Weißer, Dr. S. Mazaheri

This report summarizes the outcomes of a source code audit conducted on the KIT KASTEL Enclave flows, configurations, architecture, and threat model.

To offer context regarding the assignment's origination and composition, representatives from Karlsruher Institut für Technologie contacted Cure53 in December 2025 with the initial request. Thereafter, the active analysis period was scheduled for CW07 February 2026. The initiative was carried out by a team of five experienced consultants, who were responsible for the preparation, execution, and finalization phases. For widespread coverage levels within the expected purview of this task, the testing team was designated a workday allocation of eighteen days.

The audit setup comprised seven unique Work Packages (WPs) denoting each key area of interest, defined as follows:

- **WP1**: Architecture & threat-model review (Goals vs. Assumptions)
- **WP2**: Trust boundaries & config review (RBAC, users, privileges)
- **WP3**: Buildroot & system config review (configurations, reproducibility)
- **WP4**: Source code audit against Init & Network Init Scripts (bash)
- **WP5**: Source code audit against fork & mysetsid (C utilities)
- **WP6**: Source code audit against run-encrypt.sh, run-attest.sh, run-vm.sh
- **WP7**: Source code audit against Kernel & tboot custom-made patches

The assessment adhered to a white-box strategy, which was facilitated by the client's provision of assistive materials such as sources, documentation, and remote access to the enclave for dynamic analysis purposes. All other miscellaneous assets required for access or scope clarification were provided to support the ongoing efforts.

To facilitate a seamless engagement, all preliminary measures were completed in CW06 2026. The development and Cure53 teams shared a private Matrix channel for transparent discussions. This collaborative environment and the meticulously prepared scope were conducive to unhindered technical investigations. Cure53 maintained consistent communication through frequent status updates; however, as per the task's requirements, live reporting was not implemented.

The KIT KASTEL Enclave solution offers secure computation for extensive datasets, while VM images are utilized and executed by the corresponding server via a hypervisor. The server leverages a TPM to perform attestations regarding the configuration and software stack of the running server. Clients subsequently verify the attestation measurements upon which client-server enclave trust is established.

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

A total of sixteen security-related findings were identified following ample evaluations within the allotted time frame, categorized as three vulnerabilities and thirteen miscellaneous issues.

Identified Vulnerabilities:

- KIT-01-003 WP6: No timeout on VM execution leads to DoS (Low)
- KIT-01-004 WP6: DoS via large uncompressed archives for attestation (Medium)
- KIT-01-010 WP1/OOS: Internal nonce reuse on encrypting large messages (High)

Miscellaneous Issues:

- KIT-01-001 WP4: Hardcoded GRSECPW in initramfs repository (Info)
- KIT-01-002 WP6: Wait loops without timeout could result in DoS (Low)
- KIT-01-005 WP5: Different ways of error handling in fork and mysetsid (Info)
- KIT-01-006 WP6: No zeroizing of sha256sum file in encrypt script (Low)
- KIT-01-007 WP4: No nft filter rule for eth0 allows inbound traffic (Medium)
- KIT-01-008 WP4: Overly-permissive file permissions on kernel log and /var/run (Low)
- KIT-01-009 OOS: Post-quantum insecurity of AES-GCM-128 (Info)
- KIT-01-011 WP2: Improvable sharing on /data folder for encrypt / vm users (Low)
- KIT-01-012 OOS: Improving the key exchange (Low)
- KIT-01-013 OOS: Insufficient cryptographic agility (Low)
- KIT-01-014 WP5: Missing argument count check leads to crash (Info)
- KIT-01-015 OOS: Alternatives to AES-GCM (Info)
- KIT-01-016 OOS: Side-channel attacks and suitability of crypto libraries (Info)

In terms of the overall verdict, Cure53 garnered a very positive overall impression of the KIT KASTEL Enclave. The majority of the tickets were categorized as general weaknesses or hardening recommendations, with most WPs yielding minimal discoveries (or indeed none at all). Supporting this very positive result is the fact that no exploitable issues were discovered. The identified vulnerabilities concern either non-goals (e.g., availability, as discussed in the next paragraph) or were deemed out-of-scope (OOS) as they concern the utilized cryptography, which was not a priority target. Furthermore, all of them, with the exception of KIT-01-010, which was also independently discovered by the team of KIT at the same time as Cure53's discovery, merely constitute defense-in-depth actions, suggestions for alternative schemes, or minor improvement opportunities. Accordingly, these risks incur negligible meaningful impact on the enclave’s security proficiency or have already been addressed.

Tickets KIT-01-003, KIT-01-004, and KIT-01-002 exclusively affect the enclave’s availability. Raising and discussing these flaws with the development team verified that availability is not a core enclave objective, meaning that this aspect was not considered during the original development. As a result, the respective discoveries have been marked with a note for clarification and do not affect the enclave’s wider security posture. In similar direction, Cure53 stresses that the most significant discovered issue, namely the issue of KIT-01-010, was marked with the out-of-scope (OOS) work package, as it concerns the cryptography of the KIT enclave.

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

For WP1, Cure53 conducted an architectural review of the encompassing solution and threat model. The analysts investigated the enclave's goals with respect to the assumptions made by the system (as outlined in the audit specification document), as well as determined whether these are met by the architecture and implementation. The deployed architecture, infrastructure, runtime environment, dependencies, and operational model yielded a favorable verdict on the whole. The development team has evidently accounted for all emerging threats in such a high-secure computing environment. The development team of KIT took into account all emerging threats in such a high-secure computing environment, and the applied mitigations against any kind of attackers, even such as for example the enclave operator itself, showcase that the team of KIT went beyond standard solutions in securing computing environments. Many of the elements and components introduced in the architecture substantiate the performant defensive perimeter established for the solution, such as the data diodes and video camera surveillance.

Cure53 also sought to ascertain whether the solution fulfills the goals documented in the audit specification. The in-house team provided all requisite information to perform this research. All questions in relation to the architecture, goals, and rationale underpinning certain design decisions were answered promptly. Here, Cure53 can confidently state that the architecture and implementation meets all goals relative to the defined assumptions. For instance, those related to adversary persistence and honest users (Goal 4 and 5) have been achieved. In addition, no further side-channels were identified (Goal 1). Cure53 also believes that the system's component structure is minimal, thereby accomplishing Goal 6. The adopted cryptographic libraries are appropriate, the userspace build is reproducible, and the packages are up-to-date, realizing Goals 7, 10, and 11. Lastly, Goal 9 pertaining to the identifiability of the cryptographic enclave is attained. In summary, Cure53 is pleased to confirm that these goals are reasonable, sound, and definitively met.

With regards to Goal 3, Cure53 acknowledges that meaningful attestation was only verified from an architectural and high-level perspective. Given this context, the goal can be considered fulfilled.

In relation to Goal 8 (RBAC and user permissions), only minor non-exploitable hardening recommendations were pinpointed (KIT-01-011), thus achieving this particular objective. Concerning Goal 2, both the internal team and Cure53 confirmed that the implementation does not entirely meet the confidentiality requirements (KIT-01-010). However, the goal is still fulfilled from an architectural and design viewpoint; the construct simply fails to properly implement it. As the cryptography of the KIT enclave was deemed OOS for this assessment, the ticket was marked accordingly. The in-house team has already devised and implemented a remedial solution for this defect, underscoring their dedication to platform security.

For WP2, Cure53 estimated the trust boundaries by scrutinizing the RBAC, user, and privilege setup. The testing team probed the codebase for an array of attack vectors, including absent RBAC rules, overly permissive access controls, and privilege escalation. The enclave benefits from first-rate protection in this area, as the astute framework selection and enforcement of strict trust boundaries serve as strong protection against exploitation vectors. A hardening recommendation regarding a minor RBAC fault is detailed in ticket KIT-01-011.

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

For WP3, Cure53 inspected the buildroot and system configuration. Here, the source code was scoured for insecure configurations and default values that could assist towards attacking efforts. In correlation to results elsewhere, the consulting team did not locate any associated pitfalls, emphasizing the KIT enclave's effective safeguarding.

For WP4, Cure53 examined the init and network init scripts. The evaluation team scrutinized the network configuration for omitted firewall rules, manually scanned the initialization script for overly permissive file/folder permissions, and strove to pinpoint unnecessary capabilities on processes and mounts with non-essential options that could facilitate attack capabilities. Despite extensive endeavors, the testers only observed miscellaneous faults in this locale, reinforcing the very good overall impression. Specifically, absent nft rules for the network interfaces and excessively permissive access were noted in tickets KIT-01-007 and KIT-01-008, respectively. Pertinently, neither are exploitable due to the enclave's deployment configuration.

For WP5, Cure53 probed the custom *fork* and *mysetsid* implementations, although the investigative undertakings were unfruitful in spotting exploitable vulnerabilities or compromise pathways. The C files were explored for common associated flaws, such as out-of-bounds (OOB) situations, segmentation faults, subpar error handling, and logic shortcomings. Relevant findings include an absent argument length check (KIT-01-014) and an error handling unification suggestion (KIT-01-005). The code and functionality are structurally minimalistic, which substantially reduces the attack surface of these programs. In conclusion, the *fork.c* and *mysetsid.c* files constitute adequate and secure implementations for their intended functionality.

For WP6, Cure53 analyzed three scripts for the main userspace workflow. The research tasks yielded only a miscellaneous issue regarding absent file zeroization, in alignment to the current goals (KIT-01-006).[1] However, this avenue remains non-exploitable within the given operational mode and architecture. The scripts were reviewed for numerous abuse approaches, including (but not limited to) injection attacks via crafted input parameters, privilege escalation, broken RBAC, information or secret leakage, and logic flaws. In summary, the three scripts that comprise the main workflow are exemplary from a security perspective.

For WP7, Cure53 appraised the kernel and tboot custom patches. The complete lack of detected findings corroborates the implementation's excellent security health. It is worth mentioning that the source code was also scrutinized for common C program detriments (in correlation to WP5).

In conclusion, the KIT enclave left a great impression from a security perspective on Cure53. The testing team did not detect any exploitable vulnerabilities within the scope of the assessment and the framework is sufficiently capable of deterring major attacks and malpractices. The chosen architectural design, coupled with the installation of numerous defense-in-depth measures and sound frameworks, hardened the KIT enclave in such a way that in its current form, no issues have been found to be exploitable.

[1] KIT-01-002, KIT-01-003, and KIT-01-004 involve availability, which is not explicitly defined as a security goal. As such, these tickets are not representative of WP6.

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

The development team fixed several outstanding deficiencies following the completion of the audit, as itemized next:

Fixed Vulnerabilities:

- KIT-01-010 WP1/OOS: Internal nonce reuse on encrypting large messages (High)

Fixed Miscellaneous Issues:

- KIT-01-005 WP5: Different ways of error handling in fork and mysetsid (Info)
- KIT-01-006 WP6: No zeroizing of sha256sum file in encrypt script (Low)
- KIT-01-007 WP4: No nft filter rule for eth0 allows inbound traffic (Medium)
- KIT-01-008 WP4: Overly-permissive file permissions on kernel log and /var/run (Low)
- KIT-01-009 OOS: Post-quantum insecurity of AES-GCM-128 (Info)
- KIT-01-014 WP5: Missing argument count check leads to crash (Info)
- KIT-01-015 OOS: Alternatives to AES-GCM (Info)

Concerning KIT-01-001, the customer clarified that the password hash lacks functionality in a production environment, due to the absence of an interface for password usage. Regarding KIT-01-002, KIT-01-003, KIT-01-004, and KIT-01-012, the maintainers stated that the availability and key exchange limitations will be addressed in future iterations. KIT-01-011 is an accepted risk and will be nullified at a later date. Lastly, in relation to KIT-01-013, the customer confirmed that cryptographic agility is not an explicitly defined goal of the solution at present, while modifications to the cryptographic primitives will be handled via shipping new system versions.

Cure53 would like to thank Dr. Jeremias Mechler, Dr. Felix Dörre, and André Sperrle from the Karlsruher Institut für Technologie team for their excellent project coordination, support, and assistance, both before and during this assignment.