



our shielding . Your smart contracts, our shielding . Your smart c



shieldify



Ambire

SECURITY REVIEW

Date: February 10 2024

CONTENTS

1. About Shieldify	3
2. Disclaimer	3
3. About Ambire	3
4. Risk classification	3
4.1 Impact	3
4.2 Likelihood	3
5. Security Review Summary	4
5.1 Protocol Summary	4
5.2 Scope	4
6. Findings Summary	4

1. About Shieldify

We are Shieldify Security – Revolutionizing Web3 security. Elevating standards with top-tier reports and a unique subscription-based auditing model.

Learn more about us at shieldify.org or [@ShieldifySec](https://twitter.com/ShieldifySec).

2. Disclaimer

This security review does not guarantee bulletproof protection against a hack or exploit. Smart contracts are a novel technological feat with many known and unknown risks. The protocol, which this report is intended for, indemnifies Shieldify Security against any responsibility for any misbehavior, bugs, or exploits affecting the audited code during any part of the project's life cycle. It is also pivotal to acknowledge that modifications made to the audited code, including fixes for the issues described in this report, may introduce new problems and necessitate additional auditing.

3. About Ambire

Ambire Wallet is at the forefront of self-custodial cryptocurrency wallets, blending cutting-edge features with user-friendly design. It's built for everyone—from newcomers to seasoned crypto enthusiasts. With multiple login options and a variety of deposit methods, Ambire makes accessing and managing your crypto a breeze. Features like transaction batching and the gas tank option for pre-paying fees ensure smooth operations. Furthermore, Ambire makes transactions easy to understand with human-readable formats.

Learn more about Ambire's concept and the technicalities behind it [here](#).

4. Risk Classification

Severity	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

4.1 Impact

- **High** – results in a significant risk for the protocol's overall well-being. Affects all or most users
- **Medium** – results in a non-critical risk for the protocol affects all or only a subset of users, but is still unacceptable
- **Low** – losses will be limited but bearable – and covers vectors similar to griefing attacks that can be easily repaired

4.2 Likelihood

- **High** – almost certain to happen and highly lucrative for execution by malicious actors
- **Medium** – still relatively likely, although only conditionally possible
- **Low** – requires a unique set of circumstances and poses non-lucrative cost-of-execution to rewards ratio for the actor

5. Security Review Summary

The security assessment spanned one week, during which three security researchers from the core Shieldify team collectively dedicated 168 hours. The code exhibits exceptional professionalism and incorporates numerous best security practices and mitigations. The test coverage is extensive.

5.1 Protocol Summary

Project Name	Ambire
Repository	ambire-contracts
Type of Project	ERC-4337, Smart wallet
Audit Timeline	7 days
Review Commit Hash	2f75620a1a102b5bb1a9c3036ab57b41ac79bf0c
Fixes Review Commit Hash	N/A

5.2 Scope

The following smart contracts were in the scope of the security review:

contracts/AmbireAccount.sol	152
contracts/libs/SignatureValidator.sol	111
contracts/AmbireAccountFactory.sol	49
contracts/AmbirePaymaster.sol	39
contracts/DKIMRecoverySigValidator.sol	307
Total	658

6. Findings Summary

The security review did not identify issues of any kind. In addition to Ambire's exceptional professionalism, this outcome has been aided by the numerous solo audits and auditing competitions through which the files in the review's scope have been. We are very happy to see that there are such protocols, which prioritize security and code optimization to the fullest.

Congratulations, Ambire Team!

our shielding . Your smart contracts, our shielding . Your smart c



shieldify



Thank you!

