# Security Considerations

This page aims to give an overview of the most critical components of EUROe security. As a centralised stablecoin issuer, EUROe needs to balance between transparency and operational security and hence some topics are intentionally disregarded or abstracted.

## Technical Security

Membrane follows industry standards and modern best practices in software development, infrastructure, product management, and operations. Please refer to our Security and Bugs page for information regarding bug bounties and EUROe security.

### Smart Contract Security

EUROe smart contracts are developed by Membrane in collaboration with Equilibrium, a leading blockchain development organisation. Furthermore, all EUROe smart contracts are independently audited by recognised top-tier auditors.

You can find the full list of EUROe Stablecoin smart contracts and associated roles on the Contract Addresses page.

The stablecoin contracts have role-based access controls, as described in Architecture. While these roles are controlled by singular, non-multi-sig addresses, Membrane has implemented a multi-party computing system in the background in collaboration with Fireblocks to secure transaction signing. Furthermore, the admin and proxy owner roles, which can reassign other roles and upgrade the contract, respectively, are planned to undergo migration to a multi-sig controlled address.

### Partner Systems

EUROe customers, such as companies and foundations, have access to EUROe Partner Systems that allow them, among others, to issue and redeem EUROe for/to fiat. All EUROe Partner Systems are implemented independently of any other system in a restricted cloud environment. All our client-facing system components are subject to internal and external security reviews.

### Internal Systems

EUROe Internal Systems are used to communicate various instructions from Partner Systems and other sources to the smart contracts. EUROe Internal Systems are implemented independently of any other system in a restricted cloud environment with strict access controls. Furthermore, timelocks and multi-party signatures are required to initiate certain actions.

Furthermore, before any request from an Internal System is executed on-chain, it needs to pass through a separately implemented verification system operated by different staff members. All our internal system components are subject to internal and external security reviews.

## Operational Security

Membrane places EUROe's operational security as a top priority in everything we do. Among other measures, Membrane

- Has a thorough risk management and information security program;
- Has appointed a compliance officer to oversee the operations of the platform;
- Completes background checks for relevant personnel;
- Has implemented an internal whistleblowing program;
- Conducts regular security reviews for all our systems; and
- Requires systems and operations to adhere to a business continuity plan, which includes, for example, requirements for geographic separation.

## Third Parties

Critical EUROe technical components are mostly proprietary. Membrane relies on third parties for some parts of the system implementation. When third-party technologies are used, Membrane considers its risks as part of the business continuity plan and implements redundant systems where possible.

### Fireblocks

EUROe relies on Fireblocks' multi-party computing (MPC) technology for signing and approving transactions. In the unlikely case of Fireblocks failure, Membrane has implemented or is in the process of implementing fallbacks depending on the severity of the situation:

- If Fireblocks is temporarily unavailable, minting, burning, and token rescues will be temporarily unavailable.
- If Fireblocks goes bankrupt or is otherwise permanently incapacitated, there will be a temporary pause to minting, burning, and token rescues. Membrane has implemented a disaster recovery plan and the capability to quickly recover the system using manual methods. This will, however, reduce capacity to process EUROe transactions temporarily.
- If Fireblocks is compromised, the relevant contracts will be paused until the situation has been reviewed. We use, among other data, on-chain data to assess possible compromise of their systems.
- If Fireblocks is compromised and malicious or unauthorised transfer of funds occurs, Membrane will reinstate the EUROe balances to be honoured to the point in time immediately before the compromise.

## Blockchains

The EUROe Stablecoin is made available on various public and private blockchains. In the case of total and irrecoverable failure of the blockchain, Membrane will honour the claims at the point in time immediately before the failure. Membrane maintains access to archival nodes for all the blockchains it operates on to provide this functionality.

With respect to hacks, law enforcement orders, and forks, Membrane will evaluate the situation on a case-by-case basis.