

Forum: [Hack Forums](#)

Thread: [What is Secret Harbor? Cryptographic multi-signature transactions in Safe Wallet](#)

digital2key - October 4, 2025, 12:31 am

Many crypto teams and organizations are turning to multi-signature wallets to increase the security of their digital assets and manage their funds. By dividing responsibility among multiple signatories, these tools reduce the risk of error or unilateral abuse. However, there is a fundamental problem with this solution; since during the signing process, transaction details are placed in a public queue before being recorded on the blockchain, all their sensitive information becomes visible to everyone. Imagine a company that wants to move part of its capital into a multi-signature wallet as part of its treasury strategy; if the transaction information is visible to competitors or attackers before it is finalized, it could easily become the subject of an attack or abuse, causing serious losses.

To solve this problem, Safe Research, the developer of the Safe multi-signature wallet, has introduced a new innovation called Secret Harbour. This technology offers a new generation of decentralized transaction queues and uses end-to-end (E2EE) cryptography to ensure that transaction details remain completely confidential until the final recording on the chain. This puts privacy and security at the heart of Safe's multi-signature transaction management, eliminating the risks of information disclosure.

In the Ethereum Virtual Machine (EVM) blockchain space, multisig wallets like Safe are considered the most important security tools. The mechanism of these wallets is simple but very important; no one person can transfer funds alone, and each transaction requires the approval of multiple independent signatories. This mechanism prevents the unilateral transfer of assets and creates a strong layer of security. But it's not all about the contracts on the blockchain; part of this structure is the process of coordinating and queuing multisig transactions before they are finalized on the blockchain. To solve this issue, the Safe wallet development team initially introduced a system called Harbour. Harbour collects the necessary signatures for multisig transactions by creating a decentralized, permissionless transaction queue. By default, the system uses the Gnosis Chain as a neutral and trusted layer for data availability so that teams can exchange verified signatures with each other.

However, Harbor had a serious limitation: since the transaction queue was public, the details of all transactions were exposed to everyone. At first glance, this may not seem like a big deal, but consider a real-world scenario. Suppose an organization wants to implement its treasury strategy; if the details of these transactions are revealed before they are finalized, competitors or attackers can exploit this information to inflict heavy losses on the organization.

To address this weakness, the Safe team introduced a new innovation called Secret Harbor. This version, while maintaining Harbor's decentralized architecture, also added the crucial feature of end-to-end encryption (E2EE). This way, transaction details are only exchanged between signatories, and that too in encrypted form. More importantly, this confidentiality remains intact until the transaction is finalized on the blockchain, even if the signature collection process takes a long time.

Secret Sharing Mechanism in Secret Harbour

To understand how Secret Harbor works and how it keeps sensitive information safe, we need to look at how it is encrypted. The main goal of Secret Harbor is to ensure that transaction information is only accessible to authorized individuals, even when data is transmitted over public channels.

Key Generation

Harbor uses a mechanism called Sign-in with Ethereum to generate Deterministic Session Keys for the encryption process. These keys have several advantages over regular symmetric keys:

The key generation mechanism works in all Ethereum-compatible wallets and the user is not limited to a specific wallet.

Session keys are Deterministic. This means that they are generated in such a way that they always remain in the user's wallet and do not need to be stored in the browser or backed up.

Wallets can apply additional security checks to their domains to prevent phishing attacks.

For example, if a malicious decentralized application attempts to gain unauthorized access to Secret Harbor session keys, the SIWE-based authentication system will block it. In such a situation, even wallets like MetaMask will display a security warning similar to the image below:

This process is not entirely without its drawbacks, however, as the encryption keys are generated in the web interface of Harbor, not in hardware wallets. However, since transactions are recorded on the public blockchain and Secret Harbor supports key rotation for future transactions, the risk is significantly reduced.

Unchained Key Server

In order for end-to-end encryption to work properly in a multi-signature wallet, transaction signers must securely exchange their session keys with each other. To solve this problem, Secret Harbor acts as a Trustless Key Server, allowing any account to record its session encryption keys on the blockchain.

Each signer's session key registration is authenticated as Unchained to ensure that the transaction was encrypted with the correct recipient's public key. This eliminates the possibility of key substitution or manipulation, which is a trigger for a man-in-the-middle (MITM) attack.

Secret Harbor offers two methods for authenticating and registering keys; the signer can directly send a transaction to the Secret Harbor contract. In this case, the contract automatically registers the cryptographic key based on the msg.sender variable. In the second method, the signer must sign a message based on the ERC-712 standard; this signed message can then be published and registered on the chain without the need for permission. This method provides a smoother and simpler user experience.

What is the advantage of Secret Harbor over traditional mechanisms?

Secret Harbor is a step forward from traditional key exchange solutions such as the Linux kernel PGP key ring repository or root certificate authorities. Legacy solutions offer limited access due to permission requirements or require proving chains of trust, which is a complex task. In contrast,

Secret Harbor makes the key exchange path in the Safe multi-chain wallet decentralized, verifiable, and user-friendly by registering keys and authenticating them on-chain.

How are transactions encrypted?

Secret Harbor uses “Envelope Encryption” to securely encrypt transactions for multiple recipients. This method is done by relying only on public keys registered in Secret Harbor, without the need for additional private key exchanges. The summary of this process is as follows:

A random Data Encryption Key is generated for each transaction.

The transaction proposer receives the Key Encryption Keys, or public keys, of the signers from the Secret Harbor contract.

The transaction is symmetrically encrypted with the Data Encryption Key (DEK), and the Key Encryption Keys (KEK) are then used to asymmetric encrypt each signer's DEK.

The entire encrypted transaction, along with each signer's encrypted DEK, are sent to the Secret Harbor contract on the blockchain.

The result of this process is an “encrypted blob” that is stored on the chain and can only be decrypted by authorized recipients.