Argent Smart Wallet Specification

v1.6

May 4, 2020

1 Specifications

1.1 Introduction

The Argent wallet is an Ethereum Smart Contract based mobile wallet. The wallet's user keeps an Ethereum account (Externally Owned Account) secretly on his mobile device. This account is set as the owner of the Smart Contract. User's funds (ETH and ERC20 tokens) are stored on the Smart Contract. With that model, logic can be added to the wallet to improve both the user experience and the wallet security. For instance, the wallet is guarded, recoverable, lockable, protected by a daily limit and upgradable.

1.2 Guardians

The wallet security model is based on the ability to add Guardians. A Guardian is an account (EOA or smart contract) that has been given permission by the wallet's owner to execute certain specific operations on their wallet. In particular guardians can lock, unlock, and trigger a recovery procedure on the wallet as well as approve the execution of a large transfer to an unknown account.

We do not impose restrictions on who or what Guardians are. They can be a friend's Argent wallet, a friend's EOA, a hardware wallet, or even a paid third-party service.

Adding a Guardian is an action triggered by the wallet owner. While the first Guardian is added immediately, all subsequent additions must be confirmed after 24 hours and no longer then 36 hours after the addition was

requested. This confirmation windows ensures that a pending addition will be canceled (expire) should the wallet be locked or recovered.

Removing a Guardian is an action triggered by the wallet owner. It must always be confirmed after 24 hours and no longer then 36 hours after the removal was requested. This leaves the legitimate wallet owner enough time to notice and prevent the appointment of an illegitimate Guardian (or the dismissal of a legitimate Guardian) in case the owner lost control over their mobile device.

1.3 Locking

In case the wallet owner suspects his account (i.e. device) is compromised (lost, stolen, ...), he can ask any of his Guardians to lock the wallet for a security period of 5 days. Once the wallet is locked only a limited set of actions can be operated on the wallet, namely the recovery procedure, the unlock procedure, or the revocation of Guardians. All other operations (add guardian, assets transfer, ...) are blocked.

To unlock a wallet before the end of the security period, any guardian should trigger a wallet unlock.

1.4 Recovery

Wallet recovery is a process requested by a user who asserts ownership of a wallet while not being in possession of the owner key. A successful recovery sets a new account as the wallet owner. This process should be validated by the wallet's guardians to be executed. Once a recovery has been executed it may be finalised after 36 hours, unless it has been cancelled.

The number of signatures needed to execute a recovery is given by

$$\left\lceil \frac{n}{2} \right\rceil$$

where n is the total number of guardians and $\lceil \rceil$ is the ceiling function.

A recovery can be cancelled before finalisation. The number of signatures (owner and/or guardians) needed to cancel a recovery is given by

$$\left\lceil \frac{n+1}{2} \right\rceil$$

where n is the total number of guardians when the recovery was executed.

Once a recovery is started the wallet is automatically locked. The wallet can only be unlock by finalising or cancelling the ongoing procedure, i.e. Guardians cannot unlock during a recovery.

1.5 Ownership Transfer

In addition to recovery it is possible for a user to transfer ownership of his wallet to a new device while still being in possession of the actual phone. This transfer is immediate to avoid service interruption but must be approved by guardians. The number of required signatures is given by

$$1 + \left\lceil \frac{n}{2} \right\rceil$$

where the first signature is the owner and n is the total number of guardians.

1.6 Daily Transfer Limit

The wallet is protected by a daily limit (rolling for 24 hours). The owner can spend up to the daily limit in a given 24 hours period. The daily limit default value is 1 ETH and can be modified by the owner but it takes 24 hours for the new limit to be effective.

Any transfer exceeding the daily limit will be set as pending, and can be executed only after 24 hours.

Transfers to whitelisted addresses (see Section 1.7) and transfers approved by guardians (see Section 1.8) do not contribute to the daily limit.

The daily limit is cross-token (ETH + ERC20) and we're using an on-chain oracle to get the conversion rates for ERC20 tokens.

1.7 Whitelist

The wallet keeps a whitelist of trusted addresses. Transfers to those addresses are immediate and their amounts are not limited.

Adding an address to the whitelist is an action triggered by the wallet owner and takes 24 hours to be effective. Removing an address is triggered by the owner and is immediate.

1.8 Approved Transfer

Transfers exceeding the daily limit can be executed immediately by the owner, provided that he obtains approval from their guardians. The number of required signatures for an approved transfer is given by

$$1 + \left\lceil \frac{n}{2} \right\rceil$$

where the first signature is the owner and n is the total number of guardians.

1.9 ERC20 Exchange

The owner is able to exchange ETH against ERC20 tokens through the KyberNetwork on-chain exchange and a fee of 0,15% is charged on every transaction. The fee is paid in ETH.

Swapping tokens is not constrained by the daily limit since no value is leaving the wallet.

1.10 ENS

The Wallet is associated to an ENS. This association is forward and backward meaning that it is possible to obtain the Wallet address from the ENS and the ENS from the Wallet address.

1.11 Upgradability

The wallet is upgradable to add new features and fix potential bugs. The choice of whether to upgrade or not a wallet is left to the wallet owner. In particular, it is not possible for a centralised party such as Argent to force a wallet upgrade and change an implementation that is assumed to be immutable by the owner.

1.12 ETH-less Account

Owner and guardians can execute wallet operations without the need to pay transaction fees and own ETH, i.e. they are ETH-less account. This is achieved by enabling accounts to sign a message showing intent of execution, and allowing a third party relayer to execute the transaction and pay the fee

on their behalf. The party signing the transaction can specify if the wallet should refund the gas (partially or totally) required to execute the transaction to the third party relayer. This pattern, now called meta-transactions, is described in EIP 1077[1] and implemented in the abstract *Relayer Module* (see Section 2.4).

1.13 Summary of Guardian Operations

	Lock/Unlock	Execute Recovery	Cancel Recovery	Transfer Ownership	Approve Transfer
	Guardians	Guardians	Owner OR Guardians	Owner AND Guardians	Owner AND Guardians
1	1	1	1	2	2
2	1	1	2	2	2
3	1	2	2	3	3
4	1	2	3	3	3
5	1	3	3	4	4

Table 1: Number of signatures required to perform operations. Depending the type of the operation, signatures can be required from guardians only or by a combination of guardians and/or owner.

2 Implementation

2.1 Smart Contracts architecture

Our architecture is made up of multiple contracts (see Figure 2.1). A first group of contracts form the infrastructure required to deploy or update user wallets. These infrastructure contracts are meant to be deployed only once:

- **Multisig Wallet:** Custom-made multi-signatures wallet which is the owner of most of other infrastructure contracts. All calls on those contracts will therefore need to be approved by multiple persons.
- **Wallet Factory:** Wallet factory contract used to create proxy wallets using CREATE or CREATE2 and assign them to users.

[1] https://eips.ethereum.org/EIPS/eip-1077

- **ENS Manager:** The ENS Manager is responsible for registering ENS subdomains (e.g. mike.argent.xyz) and assigning them to wallets.

- **ENS Resolver:** The ENS Resolver keeps links between ENS subdomains and wallet addresses and allows to resolve them in both directions.

- **Module Registry:** The Module Registry maintains a list of the registered *Module* contracts that can be used with user wallets. It also maintains a list of registered *Upgrader* contracts that a user can use to migrate the modules used with their wallet (see Section 2.2).

- **Compound Registry:** Registry maintaining a mapping between underlying assets (ETH, DAI, BAT, etc) and their corresponding Compound Token (cETH, cDAI, cBAT, etc).

- **Maker Registry:** Registry maintaining a mapping between token collaterals (ETH, BAT, USDC, WBTC) and their corresponding Maker Join adapters.

- **Token Price Provider:** On-chain price oracle for ERC20 tokens. It is used by wallets to estimate the value in ETH of ERC-20 transfers and update the daily limit.

A second group of contracts implements the functionalities of the wallet:

- **Modules:** Different functionalities of the wallet are encapsulated in different modules. In general, a single module contract (e.g. *GuardianManager*) is used by all wallets to handle a specific set of operations (e.g. adding and revoking guardians). New modules can be added, existing modules can be upgraded and old modules can be deprecated by Argent. This follows a wallet design pattern recently introduced by Nick Johnson[2]: instead of directly calling a method in their wallet to perform a given operation (e.g. transfering a token), users call a method in the appropriate module contract (e.g. *transferToken()* in the *TokenTransfer* module), which verifies that the user holds the required authorization and if so, calls an appropriate method on the wallet (e.g. *invoke()*, to call an ERC20 contract).

[2]https://gist.github.com/Arachnid/a619d31f6d32757a4328a428286da186 and https://gist.github.com/Arachnid/6a5c8ff96869fbdf0736a3a7be91b84e

- **Module Storages:** Some modules store part of their states in a dedicated storage contract (see Section 2.3).
- **Proxy Wallet:** Lightweight proxy contract that delegates all calls to a Base Wallet library-like contract. There is one proxy deployed per wallet. Note that the rationale for using the Proxy-Implementation design pattern[3] is *not* to enable wallet upgradability (we use upgradable modules for that) but simply to reduce the deployment cost of each new wallet.
- **Base Wallet:** The Base Wallet is a simple library-like contract implementing basic wallet functionalities used by proxy wallets (via delegatecalls), that are not expected to ever change. These functionalities include changing the owner of the wallet, (de)authorizating modules and performing (value-carrying) internal transactions to third-party contracts.

2.2 Upgradability

Argent maintains an evolving set of registered *Module* contracts. A subset of these *Module* contracts are *SimpleUpgrader* modules that define a migration path from a particular set of old modules to a new set of registered modules, i.e. it contains the list of modules to disable and the list of modules to enable to go from the old set to the new set. A user can perform an upgrade of their modules using one of the registered *SimpleUpgrader* contracts.

2.3 Storage

In general, each module stores the entire state pertaining to all the wallets that use that module. For example, the *TransferManager* module stores how much of their daily allowance has been used by each wallet. Some modules such as *TransferManager* make use of an additional storage contract (e.g. *TransferStorage*). This is the case when their storage needs to be accessed by other modules and/or to simplify the upgradability of that module in the future.

[3]introduced by Nick Johnson in https://gist.github.com/Arachnid/4ca9da48d51e23e5cfe0f0e14dd6318f

2.4 Meta-Transactions

Meta-Transactions are implemented in the abstract *RelayerModule* from which all modules inherit. It implements a permissionless method *execute()* that is meant to be called by a relayer account. The relayer must pass to the *execute()* function an intention and the signature(s) of this intention by the originator(s) of that intention. As described in Section 1.12, this pattern allows ether-less accounts to perform operations on the wallet without the need to directly call the corresponding module methods to do so.

The RelayerModule delegates the implementation of the code that verifies the intention and the signature(s) to the subclass modules that implement it.

2.5 Modules

2.5.1 GuardianManager module

This module is used by the wallet owner to add or revoke a guardian. The addition or revokation of a guardian is done in two steps: an addition (or revokation) step that takes 24h to complete, followed by a confirmation (or cancellation) step that needs to be done in a subsequent 12h window period.

2.5.2 LockManager module

This module is used by guardians to lock or unlock a wallet.

2.5.3 RecoveryManager module

This module is used to change the owner of a wallet to a new owner. It can be executed immediately if the owner is still in possession of the current owner account (transfer ownership), or with a delay if the owner account is lost or stolen (recovery). Both operations need to be approved by guardians.

2.5.4 TransferManager module

This module lets users perform transfers of ETH and ERC20 tokens, approve ERC20 tokens for third-party contracts, or call third-party contracts directly. Calling contracts can be coupled with a value transfer by either providing an ETH amount or approving a spender to widthraw an ERC20 amount as part of the same transaction.

All transfers of value can be done either to whitelisted addresses without any limit, or to non-whitelisted addresses within a certain daily allowance. If the daily limit is reached for a given period, the transfer is set to a pending state and will only be executed after 24h.

2.5.5 ApprovedTransfer module

This module lets users perform instant transfers of ETH and ERC20 tokens, approval of ERC20 tokens, or contract calls to non-whitelisted addresses with the signed approval of a majority of guardians.

2.5.6 TokenExchanger module

This module lets users exchange ETH or ERC20 tokens for ETH or other ERC20 tokens using Kyber Network.

2.5.7 CompoundManager module

This module lets users lend and borrow tokens with the Compound protocol.

2.5.8 NftTransfer module

This module lets users transfer collectibles that comply to the ERC-721 interface.

2.5.9 MakerManagerV2 module

This module lets users invest their DAI in the DSR (Dai Savings Rate) or borrow DAI with the Maker protocol.

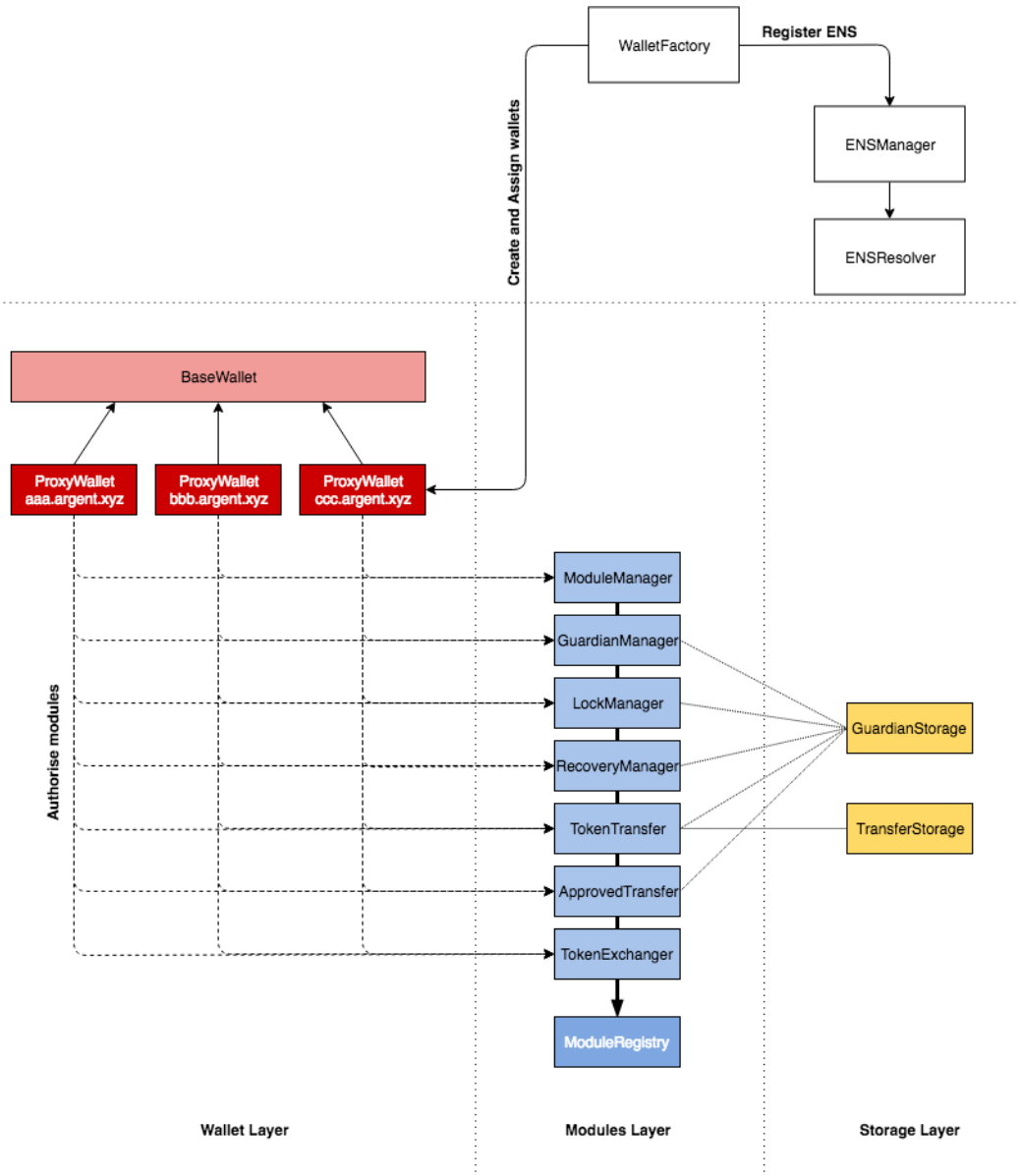

Figure 1: Smart Contracts architecture: ownership and management relationships