



# OMA3

[TIWG MVP Request for Proposals]

[WW.OMA3.ORG](http://WW.OMA3.ORG)

[INFO@OMA3.ORG](mailto:INFO@OMA3.ORG)

# 1. Introduction

This Request for Proposals (RFP) is released by OMA3's Token Working Group (TWG). The purpose of this RFP is to solicit implementation proposals for the minimum viable product of OMA3's token architecture (T-MVP). It is also a call for non-members with existing products in this area to join OMA3 and help build the T-MVP.

OMA3's token architecture was first introduced in mid-2023 with the release of its [Soulbound Token Litepaper](#). This litepaper has now been replaced with the [OMA3 Token Litepaper](#) that adds a fungible token to the foundational soulbound token.

## 2. Purpose

The purpose of this Request for Proposals (RFP) is to outline the requirements and criteria for the T-MVP and to solicit solutions (both existing and proposed) that can be used to implement the T-MVP. These solutions may come from the diverse OMA3 community of Creators, Participants and Sponsors, or outside of the OMA3 membership community.

### 3. Scope

The T-MVP is OMA3's first step into bringing its governance on-chain with software automation. It will include a fungible token that will be used in conjunction with the soulbound token, and the MVP will mint both of these tokens.

This RFP starts with a high-level “use cases” description of the T-MVP. The RFP then outlines high-level threats for circumventing the system. The RFP finally details a comprehensive range of functional and non-functional requirements that the T-MVP needs to fulfill.

It is important to note that the T-MVP is not a technical standard, so a detailed specification does not need to be written and approved by OMA3. The T-MVP may adhere to standards that OMA3 may create in the future (such as the yet-to-be-approved KYC and reputation protocol projects), but will not be a standard itself.

## 4. Use Cases

This section of the Token Working Group (TWG) Request for Proposal focuses on the use cases for the T-MVP or the “System”. This System, comprising both soulbound tokens (SBTs) and fungible tokens (FTs), is designed to facilitate various operations and programs under the OMA3 umbrella. It includes smart contracts governing SBTs and FTs, as well as the administration of bounties. It also includes a front-end website that provides web access to these contracts.

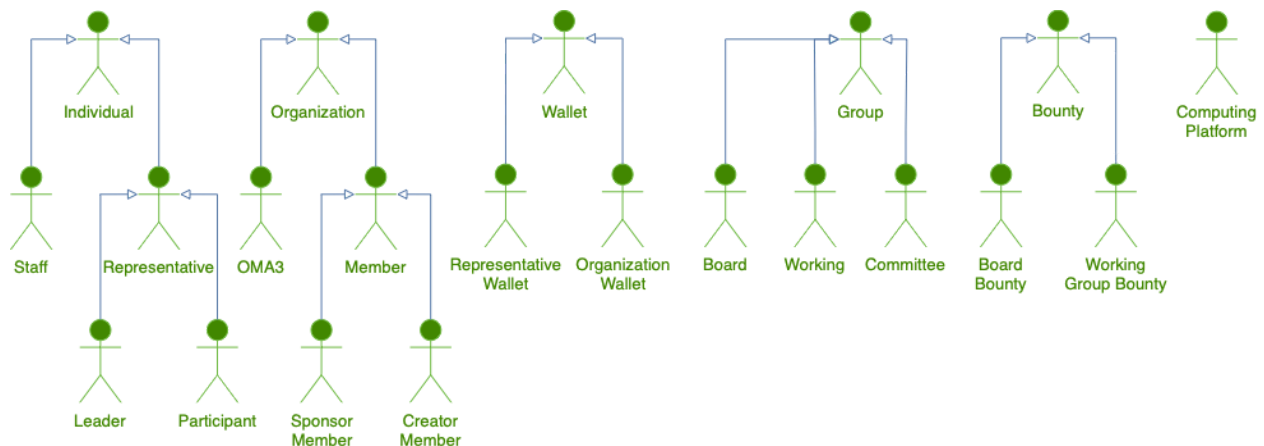
The use cases described herein are essential to understand the functional dynamics of the System. They encompass a wide range of activities, including membership management, meeting logistics, the creation and fulfillment of bounties, leadership roles, referral programs, and the overall management of fungible tokens. These scenarios provide a comprehensive view of the System's potential impact on the governance and operational efficiency of OMA3.

### Actors

In the proposed token architecture of OMA3, several key actors play integral roles interacting with the System:

- Organization: Any organization
  - OMA3: the governing body of the System.
  - Member: an Organization that is a member of OMA3, including:
    - Sponsor Members
    - Creator Members
    - Community Members
- Individual: a person.
  - Representative: Individual that works for a Member, including:
    - Leader: Representative that holds a leadership position in OMA3 such as:
      - Working Group Chair
      - Officer
      - Committee Chair
    - Participant: Representative that does not have a leadership position.
  - Staff: Employees or contractors of OMA3 or an OMA3 supplier organization

- **Wallet:** Cryptographic module that is able to perform blockchain transactions.
  - **Representative Wallet:** Wallet that is solely controlled by a Representative. A representative wallet can contain a complete private key or a part of a key (e.g.- for use in multi party computation).
  - **Organization Wallet:** Wallet controlled by an Organization that requires one or more Representative Wallets to sign transactions
- **Group:** an official decision-making body in OMA3 such as:
  - **Board:** Group that has administrative control of OMA3
  - **Working:** Group that is created by the Board for a specific task and is open to any Member except Community Members
  - **Committee:** Group that is created by the Board for a specific task, such as:
    - **Executive:** Administrative Committee
    - **Comms:** media relations Committee
    - **Finance/Warchest:** currency Committee
- **Bounty**
  - A task that rewards cash and reputation points for fulfillment.
    - **Working Group Bounty:** Bounty created by a Working Group Chair
    - **Board Bounty:** All other Bounties
- **Computing Platform-** initially Ethereum with a potential migration to one or more other chains in the future.



These actors interact with each other and the System in various ways, as outlined in the use cases that follow.

### **System Launch Use Case**

The initiation of the token architecture in the OMA3 ecosystem begins with the System Launch, which involves the following step:

1. The OMA3 Organization Wallet deploys the System's smart contracts on the selected Computing Platform.

This step sets up the infrastructure for soulbound tokens (SBTs), fungible tokens (FTs), and the bounty program.

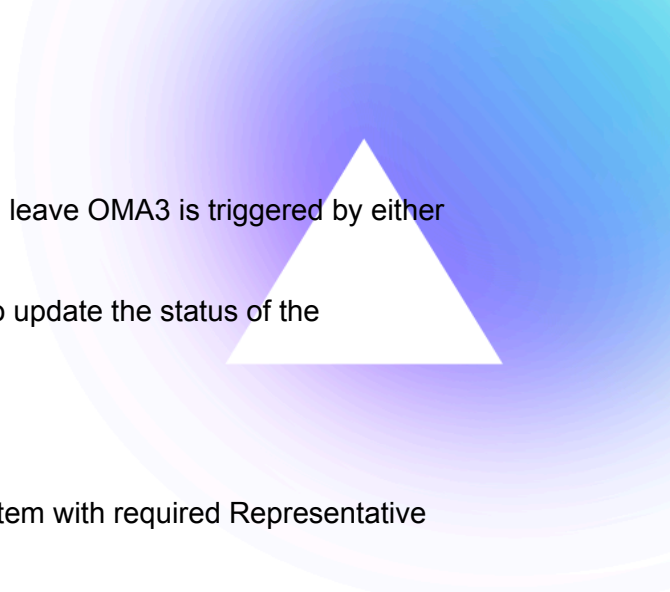
### **Membership Use Case**

The Membership use case within the T-MVP encompasses several processes and functionalities for organizations within the OMA3 ecosystem, categorized as follows:

Joining OMA3 (Creator level):

1. Application and Fee Payment: Organization completes a membership application and pays the associated fee to join OMA3.
2. KYC Process: OMA3 conducts KYC (know your customer) and (optionally) AML (anti money laundering) checks on the Organization.
3. Wallet Setup: If necessary, representatives of the Organization set up their individual Representative Wallets.
4. Organization Wallet Establishment: If necessary, the Organization establishes an Organization Wallet, configured to require signatures from multiple Representative Wallets.
5. Membership Status Update: OMA3 updates the status of the Organization Wallet in the System to reflect its membership as a Creator Member.
6. System Integration: The addresses of both the Organization and Representative Wallets are added to the System (e.g.- assigning an SBT to the Organization Wallet).

Leaving OMA3:

- 
1. Initiation of Departure: An Organization's decision to leave OMA3 is triggered by either the Organization or OMA3.
  2. Status Update in System: OMA3 uses the System to update the status of the Organization Wallet to 'Non Member'.

#### Modifying Representatives:

1. Organization Wallet adds Representative to the System with required Representative Wallet signatures.
2. Organization Wallet adds Representative to the Organization Wallet with required Representative Wallet signatures.
3. Organization Wallet removes Representative from the Organization Wallet with required Representative Wallet signatures.
4. Organization Wallet removes Representative from the System with required Representative Wallet signatures.

### **Attendance Tracking Use Case**

The Attendance Tracking use case in the TWG's proposed system is designed to manage and document participation in various meetings and events within the OMA3 ecosystem. This process is essential for ensuring accountability and active participation of members in the governance and decision-making processes. The key components of this use case include:

#### Recording Meeting Minutes and Attendance:

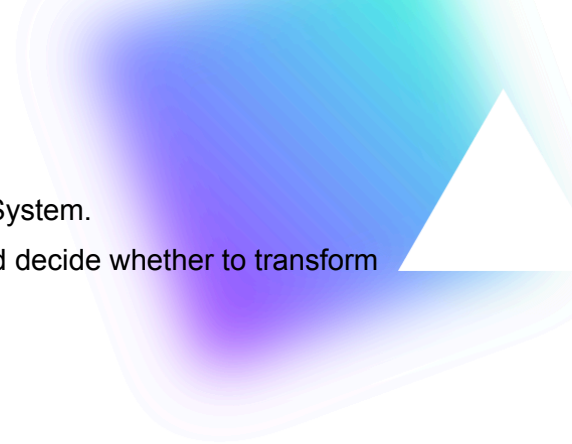
1. The Leader uses the System to record meeting minutes in the System, including which Representatives attended the Group meeting.

### **Bounties Use Case**

The Bounties use case in the T-MVP is for incentivizing and rewarding specific tasks and contributions within the OMA3 ecosystem. It encompasses various aspects of bounty creation, fulfillment, and closure:

#### Board Bounty Creation:



- 
1. Organization Wallets propose a new Board Bounty via the System.
  2. The Board then uses the System to review the proposal and decide whether to transform it into an open bounty or reject it.

#### Working Group Bounty Creation:

1. Working Group Chair creates a Working Group Bounty using the System.

#### Fulfilling Board Bounties:

1. Members view open Board Bounties in the System and submit proposals for fulfillment.
2. The Board reviews these proposals and votes on their approval, including determining the reward amounts.

#### Fulfilling Working Group Bounties:

1. Members use the System to submit proposals for open Working Group Bounties.
2. These proposals are then reviewed and voted on by the respective Working Group.

#### Closing Board Bounties:

1. The Board uses the System to close a bounty so that proposals can no longer be submitted.

#### Closing Working Group Bounties:

1. Working Group Chairs use the System to close a bounty upon completion or when it is no longer relevant.

### **Leadership Use Case**

The Leadership use case in the T-MVP outlines the processes involved in managing the leadership roles within OMA3. This includes the addition, removal, and tracking of leaders.

#### Adding Leaders:

1. Assignment of Roles: OMA3 enters a Representative into the System as a leader, including role such as Working Group Chair, Officer, or Committee Chair.

2. Token Compensation: OMA3 records any token compensation associated with these leadership positions, such as points per hour, a periodic retainer, or a fixed fee.

#### Removing Leaders:

1. OMA3 removes a Representative's leadership status in the System.

#### Tracking Hours:

1. Hour Submission: Representatives, including leaders, use System to fill out a form to input their work hours into the System.
2. Approval Process: OMA3 uses System to review and approve the submitted hours, ensuring accuracy and accountability.

### **Referrals Use Case**

The Referrals use case is designed to recognize and reward members for contributing to the growth and reach of the OMA3 ecosystem. This includes tracking and managing rewards for referrals related to press coverage and new memberships.

#### Press Referrals:

1. When a member successfully refers a press opportunity to OMA3, OMA3 records this contribution in the System with a specific Bounty amount.


#### Membership Referrals:

1. OMA3 enters the Member and the referred new member(s) into the System, including the Bounty amount.

#### Referral Edits:

1. OMA3 updates referral details in the System.
2. OMA3 and members affected by the updates can see the update transaction in the System.

### **Fungible Token Use Case**



The Fungible Token design is intended to augment the System to encourage contribution and track reputation. This section outlines the key processes and policies governing the fungible tokens:

#### Token Deployment and Allocation:

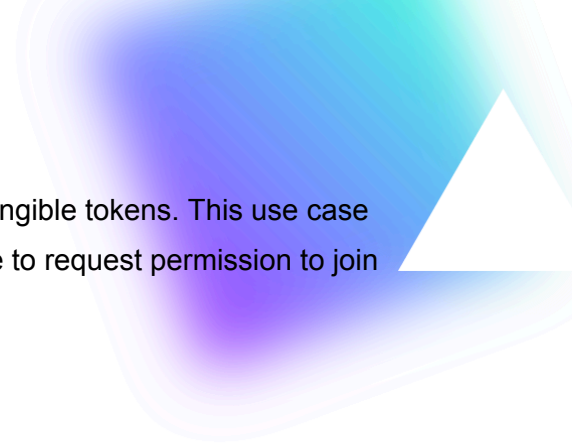
1. Smart Contract Deployment:\*\* OMA3 deploys the System's fungible token Smart Contract on the Computing Platform.
2. Distribution of Tokens: OMA3 conducts an initial distribution of fungible tokens, airdropping them to Organization Wallets. This is the token generation event (TGE).
3. Lockup Period: The System enforces a lockup period for the fungible tokens, during which the tokens cannot be transferred or traded to non-members.
4. Transfer Mechanisms: Post lockup period, Organization Wallets may transfer fungible tokens to another wallet or account via a Computing Platform.

#### **Board Staking**

For members wishing to join the OMA3 Board, a staking mechanism is implemented where members stake fungible tokens as part of their commitment to the ecosystem.

1. Member applies to join the OMA3 Board and lists the number of fungible tokens they intend to stake if they join the board.
2. Board votes to accept Member as board representative.
3. Member pays annual fee.
4. Member stakes fungible tokens.
5. Bad behavior by the Member (as defined in the Organizational Documents) may result in slashing stake based on a Board vote.

#### **Membership Staking**



In the future OMA3 may require other membership levels to hold fungible tokens. This use case flow is the same as Board Staking except members would not have to request permission to join the membership level.

1. Entity purchases fungible tokens.
2. OMA3 verifies Entity's information.
3. Optional- OMA3 issues Entity a SBT.

### **Bounty Proposal Staking**

As part of submitting a Bounty proposal, members have the option to stake a certain number of fungible tokens. This staking acts as a guarantee for their commitment to fulfilling the bounty.

1. Member uses System to stake fungible tokens with their bounty proposal.
2. Board votes to slash stake because Member did not perform bounty.
3. If the vote passes, fungible tokens are transferred to OMA3's Treasury.

### **Optional Use Cases**

OMA3 would also like to integrate the following use cases that are commonly implemented in other DAOs. These include:

- Tracking Github commits: Many DAOs reward token allocation points for committing code to repositories and
- Reposting, commenting, and liking OMA3 announcements on social media. OMA3 values Members that take the effort to amplify the OMA3 mission and its projects on social media.

There are several tools in the market that enable these use cases and OMA3 welcomes proposals from their creators.

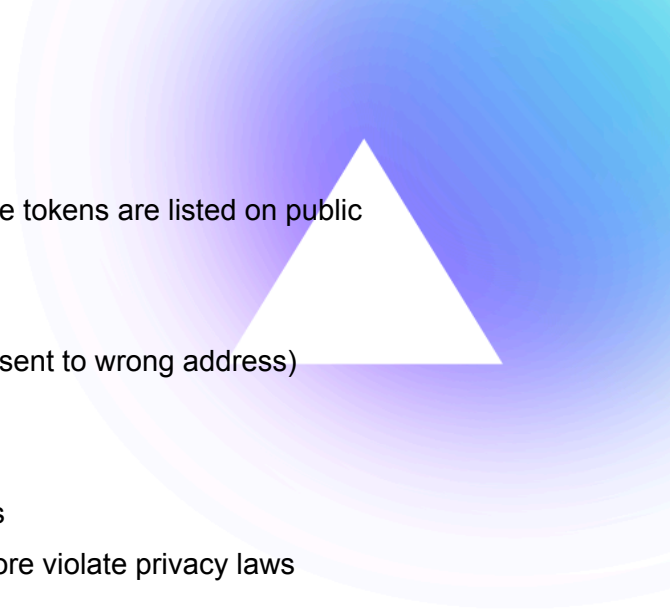
# 5. Threats

For a background on the section, read Section 4 of the [OMA3 Working Group Process](#). Threats are categorized by [use case](#).

1. System Launch
  - 1.1. Software defects found in the following components could allow a threat actor to attack the System:
    - 1.1.1. Smart contracts
    - 1.1.2. Front end
    - 1.1.3. Wallet
    - 1.1.4. Development tools
    - 1.1.5. Computing platform
  - 1.2. Malicious actors in OMA3 have administrative control of the System and could abuse this control. The two types of malicious actor threats are:
    - 1.2.1. Single malicious Individual
    - 1.2.2. Multiple malicious Individuals
2. Membership
  - 2.1. Joining OMA3
    - 2.1.1. Organization is not a legitimate organization
    - 2.1.2. Organization falsifies its information
    - 2.1.3. Organization is illegal in some manner
    - 2.1.4. Organization is under direct or indirect control of a Member
    - 2.1.5. Organization uses an unsecure Organization Wallet
    - 2.1.6. Organization is able to change membership status itself
    - 2.1.7. SBT is owned by ERC-6551 NFT account which makes membership/reputation transferable
    - 2.1.8. Representatives use an unsecure Representative Wallet
    - 2.1.9. Representatives collude to compromise Organization Wallet
    - 2.1.10. Representatives leave Member but remain Representatives in the Organization Wallet
    - 2.1.11. Representative is part of two Organizations

- 2.1.12. Representative Wallet threats
  - 2.1.12.1. Private key lost so Representative no longer has access to the Representative Wallet
  - 2.1.12.2. Private key stolen so an unauthorized individual has control of the Representative Wallet
  - 2.1.12.3. Other auth mechanism compromised, like username/password, so an unauthorized individual has control of the Representative Wallet
  - 2.1.12.4. Vendor that has admin control of the Wallet is compromised
- 2.2. Leaving OMA3
  - 2.2.1. Organization is removed from OMA3 against its will and the reason for doing so is not justified
  - 2.2.2. Organization is mistakenly removed from OMA3
- 2.3. Modifying Representatives
  - 2.3.1. Representative is removed from Organization but now the Organization does not have the minimum number of signatures required by the Organization Wallet
  - 2.3.2. Representatives are unavailable to sign a transaction
- 2.4. Third party is able to access membership data without consent of:
  - 2.4.1. OMA3
  - 2.4.2. Organization
  - 2.4.3. Representative
- 3. Attendance
  - 3.1. Meeting chair enters incorrect data
  - 3.2. Meeting chair enters transactions without approval of meeting attendees
- 4. Bounties
  - 4.1. Board Bounties
    - 4.1.1. Too many Bounty creation proposals for Board to consider
    - 4.1.2. Proposal reward not clearly understood
  - 4.2. Working Group Bounties

- 4.2.1. Chair refuses to create a necessary Bounty
    - 4.2.2. Chair inputs incorrect Bounty
  - 4.3. Bounty Approval
    - 4.3.1. Too many fulfillment proposals as Members are farming points
    - 4.3.2. Representative does not agree to be part of a Member's proposal
    - 4.3.3. Member loses expertise (e.g.- employee leaves)
    - 4.3.4. Board and Member disagree on proposal reward
    - 4.3.5. Board cannot achieve quorum necessary to approve proposal
  - 4.4. Closing Bounties
    - 4.4.1. Bounty closed too early so Members cannot propose
  - 4.5. Bounty is never completed
  - 4.6. Bounty is completed too late
  - 4.7. Bounty is completed poorly
5. Leadership
- 5.1. Leader removed from System improperly
  - 5.2. Leader enters in incorrect hours
  - 5.3. Unauthorized parties can read confidential data
6. Referrals
- 6.1. OMA3 neglects to record a referral
  - 6.2. Referral dispute between OMA3 and Member
  - 6.3. Referral dispute between two Members
  - 6.4. One Member spams the System and requests many referrals
  - 6.5. Member incorrectly claims a referral
7. Fungible Token
- 7.1. Circumvention of lockup period
  - 7.2. Selling tokens outside approved membership sandbox in the lockup period
  - 7.3. Dumping tokens and crashing the price
  - 7.4. Fluctuating market value changes stake value

- 
- 7.5. Members need to acquire more tokens before tokens are listed on public exchanges
  - 7.6. Token holders circumvent AML/KYC checks
  - 7.7. Orphaned tokens (lost wallet keys or tokens sent to wrong address)
  - 7.8. Stolen tokens
  - 7.9. Privacy
    - 7.9.1. KYC'd wallets are not pseudonymous
    - 7.9.2. All transactions are public and therefore violate privacy laws
  - 8. Staking
    - 8.1. Board staking: Board unfairly slashes a Member's stake
    - 8.2. Bounty staking: Board unfairly slashes a Member's stake
  - 9. Optional Use Cases
    - 9.1. Not all Github commits are created equal
    - 9.2. Members have vastly differing levels of influence on social media

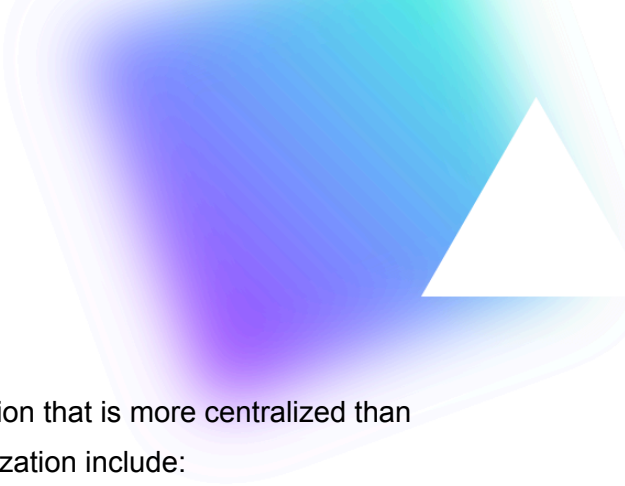


# 6. Requirements

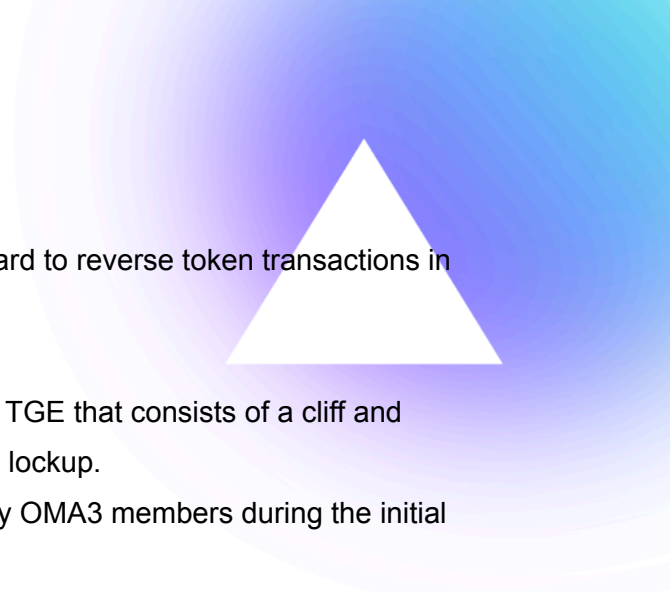
This section lists the high-level requirements derived from the use cases and threats.

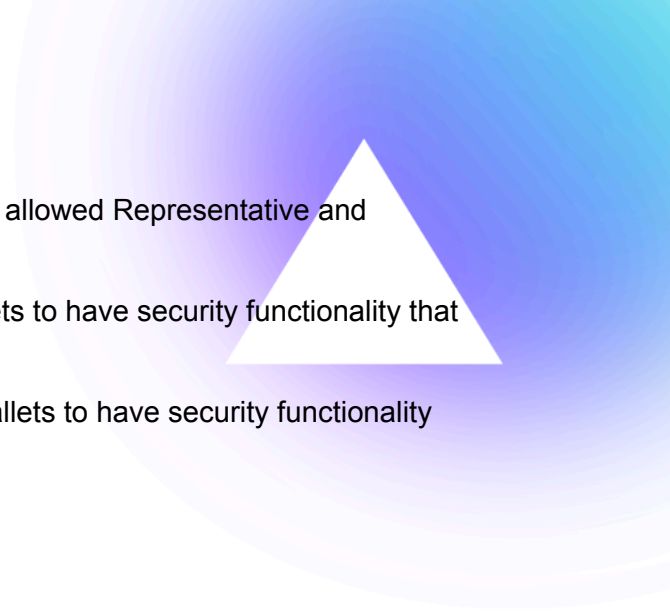
Terminology definitions can be found in Section 5 of the [OMA3 Working Group Process document](#).

1. The Computing Platform the System is deployed on:
  - 1.1. SHOULD be EVM compatible.
  - 1.2. SHALL be interoperable with other ecosystem assets like the OMA3 fungible token.
  - 1.3. SHOULD also host the OMA3 fungible token.
  - 1.4. SHALL have gas fees that do not preclude OMA3 use cases such as the Inter World Portaling System (e.g.- gas fees are too high to make the infrastructure usable)
  - 1.5. SHALL minimize the regulatory compliance effort of launching a fungible token such as reporting, taxes and KYC.
  - 1.6. MAY KYC all participants using a user-controlled, privacy-preserving reputation protocol.
  - 1.7. SHOULD offer interoperability with infrastructure OMA3 members use (e.g.- chains such as EOS, WAX, Polygon, and Chromia) for future OMA3 projects that integrate the fungible token.
  - 1.8. SHOULD NOT allow OMA3 applications to be adversely impacted by other applications running on the same infrastructure.
  - 1.9. SHALL by production ready in 2024.
  - 1.10. SHOULD offer tools that minimize the engineering and maintenance effort of OMA3.
  - 1.11. MAY offer a migration path that allows quick time to market in 2024 and satisfaction of other requirements over time.
  - 1.12. MAY have existing liquidity to hasten usage growth.
  - 1.13. SHOULD be “battle tested” for all components related to security, such as:

- 
- 1.13.1. Virtual machine
    - 1.13.2. Consensus protocol
    - 1.13.3. Hardware wallets
    - 1.13.4. Multisig wallets
  - 1.14. SHOULD NOT have a single point of centralization that is more centralized than OMA3's governance. Possible points of centralization include:
    - 1.14.1. Sequencer
    - 1.14.2. Data availability layer
    - 1.14.3. Settlement layer
  - 1.15. SHOULD NOT have a single point of centralization with governance that could be adverse to OMA3's interests.
2. Privacy
- 2.1. The System SHALL allow the public to see the following information:
    - 2.1.1. Membership status
  - 2.2. The System SHOULD keep the following information confidential to OMA3 members only:
    - 2.2.1. Leadership contribution amounts
    - 2.2.2. Contributions
    - 2.2.3. Attendance (including showing up 10 minutes late or more)
    - 2.2.4. Referrals
    - 2.2.5. Rejected bounties
    - 2.2.6. Rejected referrals
    - 2.2.7. Total contribution amount of each member prior to airdrop
    - 2.2.8. Adoption metrics prior to airdrop
    - 2.2.9. Overall reputation score
  - 2.3. The System SHOULD allow a member to give third-party access to the member's information:
3. Security
- 3.1. The System SHALL ensure System soul-bound tokens cannot be transferred from the Organization Wallet
  - 3.2. The System SHALL control which entity is associated with an Organization Wallet

- 3.3. The System SHALL ensure all Organizations are legitimate organizations.
- 3.4. The System SHALL ensure all Organizations that are under common control with another Member only have one vote.
- 3.5. The System SHALL ensure all Representatives and Individual Members do not violate Swiss sanctions laws.
- 3.6. The System MAY verify the identity of all Individual Members.
- 3.7. The System SHALL require voting adheres to the following characteristics:
  - 3.7.1. Members cannot vote twice on the same motion, bounty, or any other decision.
  - 3.7.2. Third parties cannot cast a vote for the Member.
  - 3.7.3. Censure resistant- Third parties cannot prevent a Member from voting.
- 3.8. The System SHALL require the reputation system adhere to the following characteristics:
  - 3.8.1. Members cannot modify their reputation score using methods other than what is described in the use cases document.
  - 3.8.2. Third parties cannot modify the reputation score or reputation data of a current or past OMA3 Member.
- 3.9. The System SHOULD allow a Member to recover their stolen member identity (either SBT or Organizational Wallet).
- 3.10. The System SHOULD be resistant to a rogue Representative.
- 3.11. The System SHOULD give OMA3 or Support the ability to correct events that factor into reputation or contributions.
- 4. Application
  - 4.1. The System SHALL support all use cases listed in this document.
  - 4.2. The System SHOULD address all threats listed in this document.
  - 4.3. The System SHOULD use proven existing standards and code bases when possible.
- 5. User Interface
  - 5.1. The System SHOULD be easy to understand for new Members.
  - 5.2. The System SHOULD adhere to Web Content Accessibility Guidelines (WCAG).
  - 5.3. The System MAY use dynamic NFTs (NFTs that are able to change data or metadata).

- 
6. Usability
    - 6.1. The System MAY allow an OMA3 judicial board to reverse token transactions in case of wrong-doing
  7. System Fungible Token (FT)
    - 7.1. The FT SHALL support a lockup period after TGE that consists of a cliff and subsequent linear release of tokens from the lockup.
    - 7.2. The FT SHALL only be allowed to be used by OMA3 members during the initial lockup period
    - 7.3. The FT SHOULD support different characteristics, including lockup periods and staking, for different issuance categories of token holders (e.g.- founders vs contributors).
    - 7.4. The FT SHOULD allow staking use cases during the lockup period.
    - 7.5. The FT smart contract SHOULD be upgradeable using a recognized standard (e.g.- ERC-1822).
    - 7.6. The FT upgrade capability SHOULD have the ability to become immutable in the future.
    - 7.7. The FT SHOULD support multisig controlled by a voting body of OMA3 for all development and deployment operations.
    - 7.8. The FT SHOULD support available tools that can migrate the FT to another chain.
    - 7.9. The FT SHOULD have the ability to become the native token on another chain.
    - 7.10. The FT SHOULD have a limited supply.
    - 7.11. The FT SHALL support use by all members' platforms
    - 7.12. The FT SHOULD support swaps with all members' tokens
    - 7.13. The FT MAY allow OMA3 to reverse transfers via a judicial process that MAY charge a fee to the initiating party
    - 7.14. The FT MAY support an existing cross-chain standard format.
    - 7.15. The FT MAY require KYC for any wallet that holds the FT.
    - 7.16. The FT MAY keep FT transaction data private to the parties involved.
    - 7.17. OMA3 MAY take a similar role to the FT that Circle plays with USDC across multiple blockchains.
  8. Wallets

- 
- 8.1. The System SHOULD maintain a whitelist of allowed Representative and Organization Wallets.
  - 8.2. The System MAY require Organization Wallets to have security functionality that prevents wallet threats.
  - 8.3. The System MAY require Representative Wallets to have security functionality that prevents wallet threats.



[WWW.OMA3.ORG](http://WWW.OMA3.ORG)

[INFO@OMA3.ORG](mailto:INFO@OMA3.ORG)