

# Emoney Token Standard

## Section 1: Summary

Use Case Summary			
<b>Use Case ID:</b>	FIN-008	<b>Use Case Type:</b>	<i>Vertical</i>
<b>Submission Date:</b>	July 19, 2019	<b>Is Use Case supporting SDGs</b>	<i>Yes</i>
<b>Use Case Title:</b>	Emoney Token Standard	<b>Domain:</b>	<i>1</i>
<b>Status of Case</b>	<i>In Production, ready.</i>	<b>Sub-Domain</b>	<i>B-</i> International & interbank payments
<b>Contact information of person submitting/managing the use-case</b>	<i>Full Name: Ismael Arribas</i> <i>Web site: <a href="https://emoneytokenstandard.org/standards@alastria.io">https://emoneytokenstandard.org/standards@alastria.io</a></i>		
<b>Proposing Organization</b>	<b>Iobuilders</b> (Kingdom of Spain). B-88104054		
<b>Short Description</b>	A proposed standard for e-money, bank and central bank money issued tokens		
<b>Long description</b>	<p>Financial institutions work today with electronic systems which hold account balances in databases on core banking systems. In order for an institution to be allowed to maintain records of client balances segregated and available for clients, such institution must be regulated under a known legal framework and must possess a license to do so. Maintaining a license under regulatory supervision entails ensuring compliance (i.e. performing KYC on all clients and ensuring good AML practices before allowing transactions) and demonstrating technical and operational solvency through periodic audits, so clients depositing funds with the institution can rest assured that their money is safe</p> <p>here are only a number of potential regulatory license frameworks that allow institutions to issue and hold money balances for customers (be it retail corporate or institutional types). The most important and practical ones are three:</p> <p>Electronic money entities: these are legally regulated vehicles that are mostly used today for cash and payments services, instead of more complex financial services. For example prepaid cards or online payment systems such as PayPal run on such schemes. In most jurisdictions, electronic money balances are required to be 100% backed by assets, which often entails holding cash on an omnibus account at a bank with 100% of the funds issued to clients in the electronic money ledger</p>		

Banking licenses: these include commercial and investment banks, which segregate client funds using current and other type of accounts implemented on core banking systems. Banks can create money by lending to clients, so bank money can be backed by promises to pay and other illiquid assets

Central banks: central banks hold balances for banks in RTGS systems, similar to core banking systems but with much more restricted yet critical functionality. Central banks create money by lending it to banks, which pledge their assets to central banks as a lender of last resort for an official interest rate

Regulations for all these types of electronic money are local, i.e. only valid for each jurisdiction and not valid in others. And regulations can vary dramatically in different jurisdictions - for example there are places with no electronic money frameworks, on everything has to be done through banking licenses or directly with a central bank. But in all cases compliance with existing regulation needs to be ensured, in particular:

Know Your Customer (KYC): the institution needs to identify the client before providing them with the possibility of depositing money or transact. In different jurisdictions and for different types of licenses there are different levels of balance and activity that can be allowed for different levels of KYC. For example, low KYC requirements with little checks or even no checks at all can usually be acceptable in many jurisdictions if cash-in balances are kept low (i.e. hundreds of dollars)

Anti Money Laundering (AML): the institution needs to perform checks of parties transacting with its clients, typically checking against black lists and doing sanction screening, most notably in the context of international transactions

Beyond cash, financial instruments such as equities or bonds are also registered in electronic systems in most cases, although all these systems and the bank accounting systems are only connected through rudimentary messaging means, which leads to the need for reconciliations and manual management in many cases. Cash systems to provide settlement of transactions in the capital markets are not well connected to the transactional systems, and often entail delays and settlement risk.

The EM Token builds on Ethereum ( Corda and others is under study), standards currently in use such as ERC20, but it extends them to provide few key additional pieces of functionality, needed in the regulated financial world:

Compliance: EM Tokens implement a set of methods to check in advance whether user-initiated transactions can be done from a compliance point of view. Implementations must require that these methods return a positive answer before executing the transaction

	<p>Clearing: In addition to the standard ERC20 `transfer` method, EM Token provides a way to submit transfers that need to be cleared by the token issuing authority offchain. These transfers are then executed in two steps: 1. transfers are ordered 1. after clearing them, transfers are executed or rejected by the operator of the token contract</p> <p>Holds: token balances can be put on hold, which will make the held amount unavailable for further use until the hold is resolved (i.e. either executed or released). Holds have a payer, a payee, and a notary who is in charge of resolving the hold. Holds also implement expiration periods, after which anyone can release the hold Holds are similar to escrows in that are firm and lead to final settlement. Holds can also be used to implement collateralization</p> <p>Funding requests: users can request for a wallet to be funded by calling the smart contract and attaching a debit instruction string. The tokenizer reads this request, interprets the debit instructions, and triggers a transfer in the bank ledger to initiate the tokenization process</p> <p>Payouts : users can request payouts by calling the smart contract and attaching a payment instruction string. The (de)tokenizer reads this request, interprets the payment instructions, and triggers the transfer of funds (typically from the omnibus account) into the destination account, if possible. Note that a redemption request is an special type of payout in which the destination (bank) account for the payout is the bank account linked to the token wallet</p> <p>The EM Token is thus different from other tokens commonly referred to as "stable coins" in that it is designed to be issued, burnt and made available to users in a compliant manner (i.e. with full KYC and AML compliance) through a licensed vehicle (an electronic money entity, a bank, or a central bank), and in that it provides the additional functionality described above so it can be used by other smart contracts implementing more complex financial applications such as interbank payments, supply chain finance instruments, or the creation of EM-Token denominated bonds and equities with automatic delivery-vs-payment</p>		
<b>SDG in Focus (when applicable)</b>	<i>SDG9 and SDG17</i>		
<b>Value Transfer:</b>	<b>We will transfer claims off-chain with on-chain proofs. Ponderation of attributes by causality. Verified authority to attest and authenticate an attribute.</b>	<b>Number of Users:</b>	First Po will happen in Spain (>45MM) but this solution aims to establish a global Identity system as an interplanetary badge. European Population and LAC.
<b>Types of Users:</b>	<b>People, Organizations, E.money entities, Banks, Central Banks</b>		

<b>Stakeholders</b>	<i>As we are proposing a money standards issuer and token holders are involved, that means any stakeholder is applied,</i>
<b>Data:</b>	<p><a href="https://github.com/ethereum/EIPs/pull/2020">https://github.com/ethereum/EIPs/pull/2020</a>  <a href="https://emoneytokenstandard.org">https://emoneytokenstandard.org</a></p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>All the data flow is fully detailed at</p> <p><a href="https://github.com/IOBuilders/holdable-token">https://github.com/IOBuilders/holdable-token</a></p> <p><a href="https://github.com/IOBuilders/payoutable-token">https://github.com/IOBuilders/payoutable-token</a></p> <p><a href="https://github.com/IOBuilders/clearable-token">https://github.com/IOBuilders/clearable-token</a></p> <p><a href="https://github.com/IOBuilders/fundable-token">https://github.com/IOBuilders/fundable-token</a></p> </div> <p>Privacy by design: unlinkable actions.</p>
<b>Identification:</b>	<p><i>On next releases the idea is to link the identity to SSI schemas. Having said that all the information, balances, accumulates etc, want to be kept confidential. The standard workgroup is actively working on a confidential token approach, researching and implementing homomorphic encryption, range proofs, and pedersen commitments.</i></p> <p><a href="https://crypto.stanford.edu/bulletproofs/">https://crypto.stanford.edu/bulletproofs/</a></p>
<b>Predicted Outcomes:</b>	<p><a href="https://ourion.io">Ourion.io</a> ( IOBuilders project) is already live and shows a production ready application, working under the Alastria network, managing real tokenized euros. Other uses cases have deployed under Pegasys Pantheon and JP Morgan Quorum based networks.</p> <p>Adhara, has already deployed the standard under a Singapore, Philippines payment corridor project.</p> <p>Adhara is going to deploy a use case with the South African Reserve Bank in Q4 2019.</p> <p>IOBuilders is going to deploy a use case with the BME, the Spanish CSD, on a bond issuing platform in Q4 2019.</p>

<b>Overview of the Business Problem or Opportunity</b>
Blockchain technology is starting to be seen with huge potential to speed up the the fintech innovation. Banks and financial institutions, are envisioning smart money and payments scenarios leveraged by blockchain and smart execution. To enable fully regulated payment scenarios, with

fiat tokenized money, tokens must be issued under e-money/ bank / central bank rules, and directives.

Standardization is key to enable interoperability and cross use case integration. The standard has been started and developed with the aim of enable global interoperability, on tokenized fiat money issuances and payments..

### **Why Distributed Ledger Technology?**

Advantages of fiat money tokenization on the blockchain are as following:

- Use of the universal blockchain protocol based on a continuous and interconnected chain of blocks that provides unification and universality of interactions for various market participants;
- High level of security due to inability to post-factum change the chain of blocks / tamper proof)
- Token issuers can directly communicate with parties interested in any payment use case
- Traceability
- Unique source of truth
- Auditability and transparency (by regulators)

## **Section 2: Current process**

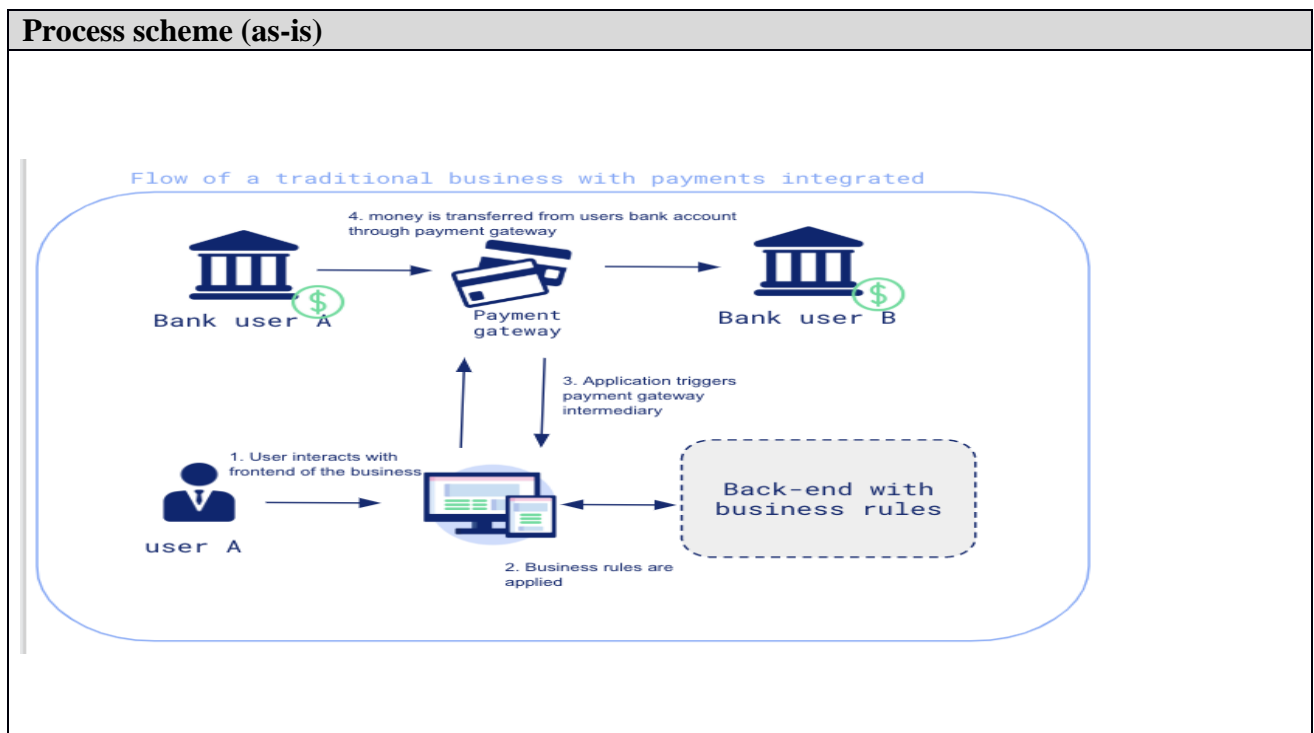
### **Current Solutions**

On [Eurion.io](https://eurion.io) lowest KYC level, has been implemented, allowing to have a yearly 1000 € limit and 250 per operation

### **Existing Flow (as-is)**

<b>Step</b>	<b>User Actions</b>	<b>System Actions</b>
1.	User Identification (KYC)	As money holders, all users need to be identified. Either central banks, banks or e-money entities need to identify users, following the established KYC rules. Based on the level of identification, users are able to manage different amounts of money.
2.	Cashin	Cashin is done via the banking system, either using payment gateways or SEPA, SWIFT communication

Existing Flow (as-is)		
Step	User Actions	System Actions
3.	Transfer	SEPA, SWIFT communication based on ISO 20022 payments standards and bank integrations
4,	Transfer with Hold	SEPA, SWIFT communication with ISO 20022 payments standards and bank integrations
5.	Cashout	SEPA, SWIFT communication with ISO20022 payments standards and bank integrations



Data and information (as-is)		
Data	Type	Description
1	<i>Documents</i>	All the identification process has important documents associated: KYC0: OTP validated mobile phone KYC1: Validated ID document KYC2: Biometric patterns linked to ID, income data, and personal IBAN Information KYC4: KYC template
2	<i>Payment transactions</i>	Cashin, Transfer and cashout

Participants and their roles (as-is)		
Actor	Type/Role	Description
1	<i>Lawyers</i>	Kyc and AML process definition
2	<i>Bank, Central Bank, and Emoney License</i>	Money issuer
3	<i>User</i>	Money holder
4	<i>Clearing Agent</i>	Allows a clearable operation to be fulfilled

Other Notes
<i>No.</i>

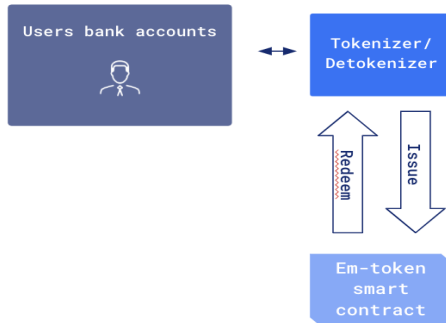
### **Section 3: Expected process**

<b>Expected Flow (TO BE)</b>		
<b>Step</b>	<b>User Actions</b>	<b>System Actions</b>
1.	User Identification (KYC)	As money holders, all users need to be identified. Either central banks, banks or e-money entities need to identify users, following the established KYC rules. Based on the level of identification, users are able to manage different amounts of money. On Eurion.io lowest KYC level, has been implements, allowing to have a yearly 1000 € limit and 250 per operation. On chain configuration is done via EIP 2009
2.	Cashin	<p>Once users have been identified, they can start using tokenized cash. There are 2 ways of being able to receive tokenized money, via an existing user that natively transfers money, or via baking system based cashin operation, either via credit card or SEPA transfer. All Eurion users, have an unique IBAN associated to its ethereum address.</p> <p>This cashin operation, can be executed on a centralized or decentralized way, via the funding method provided by the standard. On invocation, the token issuer, will read the payment transaction and mint the required tokens (EIP 2019)</p>
3.	Transfer	A native transfer between token holders.
4,	Transfer with Hold	In some cases, native transfer want to be validate or cleared by a third party, On this case mixing the hold and clearing capabilities of the standard, such kind of transactions can be easily implemented.(EIP 2019)
5.	Cashout	An cashout operation, can be executed on a centralized or decentralized way, via the payout method provided by the standard. On invocation, the token issuer, will read the payment transaction and burn the required tokens. (EIP 2021)



## Process scheme (to-be)

### Money tokenization explanation



- When money reaches the account of a user of ioCash, the bank/EME notifies us.
- The tokenizer issues the corresponding amount of tokens over the decentralized ledger into our Em-token smart contract
- Now, money is digital, programmable and interoperable
- When the user orders a redemption, the detokenizer burns the tokens on the smart contract
- Money is moved from the client ioCash account to the destination

Participants and their roles		
Actor	Type/Role	Description
1	Lawyers	Kyc and AML process definition
2	Bank, Central Bank, and Emoney License	Money issuer
3	User	Money holder
4	Clearing Agent	Allows a clearable operation to be fulfilled
5	Hold Operator	Allows a held operation to be fulfilled

Data and information		
Data	Type	Description
1	Documents	<p>All the identification process has important documents associated:</p> <p>KYC0: OTP validated mobile phone</p> <p>KYC1: Validated ID document</p> <p>KYC2: Biometric patterns linked to ID, income data, and personal IBAN Information</p> <p>KYC4: KYC template</p>
2	Payment transactions	Cashin, Transfer and cashout

### Security and privacy

*All the standard is based on current ethereum capabilities and ourion.io has been developed following all the security and ISO standards and specifications.*

### Main Success Scenario + expected time line

[Ourion.io](#) ( IoBuilders project) is already live and shows a production ready application, working under the [Alastria](#) Ecosystem, managing real tokenized euros. Other uses cases have deployed under Pegasys Pantheon and JP Morgan Quorum based networks.

[Adhara](#), has already deployed the standard under a Singapore, Philippines payment corridor project.

Adhara is going to deploy a use case with the South African Reserve Bank in Q4 2019.

[IoBuilders](#) is going to deploy a use case with the BME, the Spanish CSD, on a bond issuing platform in Q4 2019.

### Conditions (pre- or post-)

*Non applicable.*

### Performance needs

*Current Ethereum landscape is totally focused on scalability, due the low transnationality, throughput available either on private or public networks..*

### Legal considerations

*Electronic Money License, Anti-money laundering compliance and KYC regulation.*

### Risks

*Scalability and confidentiality. (mentioned before)*

### Special Requirements

*Financial institutions share a common platform and data overview.*

### External References and Miscellaneous

<https://io.cash/product/>

### Other Notes

*It is possible to be tested for free by the ITU-T FG DLT experts and members.*

## **Appendix 1:** **Domains and subdomains for use cases categorization**

### **Vertical:**

1. Finance
  - a. Financial management & accounting
  - b. International & interbank payments
  - c. Clearing and settlement
  - d. Reduction of Fraud
  - e. Financial messaging
  - f. Asset lifecycles and history
  - g. Trade finance
  - h. Regulatory compliance & audit
  - i. AML/KYC
  - j. Insurance
  - k. Peer-to-peer transactions
2. Healthcare
  - a. Pharma
  - b. Biotechnology
  - c. Medicine
3. Industries
  - a. Manufacturing
  - b. Energy
  - c. Chemical
  - d. Retail
  - e. Real estate
  - f. IT and telco
  - g. Supply chain management
  - h. Transportation
  - i. Agriculture
4. Government and public sector
  - a. Taxes
  - b. Government and non-profit transparency
  - c. Legislation, compliance & regulatory oversight
  - d. Voting
  - e. Taxation and customs
  - f. Intellectual property management
  - g. Land Registries

### **Horizontal:**

1. Identity management
2. Security management
  - a. Public Key Infrastructure
3. Internet of Things

4. Data processing, storage and management
    - a. Data Validation (includes provenance)
-