Tokenized KYC: Enhancing Compliance with IOTA
Bringing **Safety** and **Security** to DeFi

Upcoming crypto regulations will enforce stringent **Know Your Customer (KYC)** and **Anti-Money Laundering (AML)** measures. However, despite its innovations, **Decentralized Finance (DeFi)** lacks robust user authentication tools, making it difficult to establish identity on the blockchain when required. To tackle this issue, the IOTA Foundation is collaborating with **walt.id, IDnow, Bloom Wallet**, and **HAVN** on a KYC solution. It uses **tokenization** for efficient and secure **authentication** in Web3 apps, ensuring **compliance** while respecting **user privacy**.
The **Challenges** Facing Authentication

**GDPR versus KYC/AML**

Under the General Data Protection Regulation (GDPR) established by the European Commission, personally identifiable information (PII) should not be stored on the blockchain, irrespective of whether it is direct, hashed, or encrypted, due to the impossibility of deletion. However, within DeFi, there is a regulatory requirement for obliged entities to be able to track the identities of those engaged in transactions.

**On-Chain versus Off-Chain**

Decentralized off-chain systems, such as Self-Sovereign Identity, offer viable solutions for identity verification. Yet, for smart contract-based decentralized applications (dApps) to function optimally, there is also a need for on-chain authentication processes. This dual approach ensures both the efficacy of dApps and the integrity of identity management across blockchain networks.
Know Your Customer (KYC)

KYC represents the foundational phase of AML due diligence. During this process, obliged entities – individuals or organizations legally required to comply with AML rules – must gather identifying information from customers. This includes the customer's name, date of birth, address, and national identification number.

Anti-Money Laundering (AML)

AML regulations mandate that obliged entities monitor customer transactions, report any suspicious activities, and verify the identities of their customers. Our KYC solution equips these entities with the necessary data points to extend these requirements to self-hosted wallets effectively.

Transfer of Funds Regulation (TFR)

Transactions involving Crypto Asset Service Providers (CASPs) must carry identifying data about the transaction's originator and beneficiary. The identities behind self-hosted wallets must also be ascertainable. Our solution enables CASPs and other obliged entities to identify the users of self-hosted wallets through a dedicated KYC chain, which ensures that each wallet address is both identified and authenticated.
How Our **KYC** Solution Works

Our KYC solution involves a **trusted party** that **tokenizes the identification process** it has verified. This allows decentralized applications (dApps) and other entities to trust the integrity of the identification process **without disclosing any personally identifiable information**. The token generated from this process is a **soulbound token**, designed specifically for on-chain activities to facilitate Web3-native interactions.

In situations where identity disclosure is legally required, such as requests from law enforcement, the trusted party is capable of providing the necessary **identity information**. Additionally, the trusted party holds the authority to **revoke the token** under specific circumstances, such as when a token invalidation is necessary due to updates in watchlist status or similar compliance changes.
An Identification Tool for DeFi

The IOTA EVM provides an EVM-compatible smart contract chain anchored to the IOTA mainnet. DeFi protocols and other dApps are deployed on the IOTA EVM.

The authentication process is tokenized and verified. The resulting KYC token can be shared between applications. dApps can check for the presence of the KYC token in the user's address and allow or deny access to parts of their App.
User Flow

1. Sign in to dApp
2. Redirect to compliance service
3. Sign in to compliance service
4. Run through identity verification
5. Receive token
6. Receive Verifiable Credential (optional)
7. Go back to dApp
8. Sign in to dApp and proceed

https://walt.xyz/
Process Flow

IOTA provides the foundational network infrastructure for the KYC solution.

IDnow conducts the remote identification process, complying with EU AML/Countering the Financing of Terrorism (CFT) regulations and the upcoming Transfer of Funds Regulation (ToFR).

Following verification, Walt.id tokenizes the identification process, enabling decentralized applications (dApps) to confirm that a legitimate identification has taken place.

The resultant token is then securely stored in the user's Bloom Wallet, or another compatible wallet, and is soulbound to the authenticated address.

HAVN ensures that users have been appropriately identified and possess the necessary KYC token before they can use the service.

The token can be used for on-chain processes, facilitating Web3-native interactions while ensuring the user has been authenticated without revealing personal information at this stage.
Soulbound Token
Revocable and Non-Transferable

Innovative Technology Deployment

Utilizing cutting-edge distributed ledger technology, our system ensures that authentication is unequivocally linked to a single address, allowing for the potential revocation of previously issued tokens by authorized entities.

Revocable and Non-Transferable

The soulbound token represents a pioneering approach to identity verification and management within the digital sphere. It guarantees privacy and adheres to stringent regulatory standards. Each token is irrevocably bound to a specific user's authenticated address, rendering it non-transferable and intrinsically linked to the identity of its holder. This ensures that the token remains a secure and private credential that cannot be misused or transferred, upholding the integrity of user identities in Web3 environments.
Positioning **DeFi** for Mainstream **Adoption** with a Pioneering **KYC Solution**

**Privacy Preserving**
Our commitment to maintaining the confidentiality of user data is crucial in building trust and facilitating wider acceptance of DeFi platforms.

**Efficiency and Reusability**
Our system presents a significant time-saving feature with a competitive edge over traditional financial systems. The reusability of these tokens across various platforms eliminates redundant verifications, streamlining operations for users and institutions alike.

**User-Friendly Interface**
The simplicity and ease of use for all stakeholders involved enhances user experience and accessibility.

**Seamless Integration**
Our solution offers straightforward integration with dApps, reducing the technical barrier for developers and accelerating the deployment of new services within the DeFi ecosystem.

**Regulatory Compliance**
We enable dApps to document and prove that they only interact with users whose identity has been verified, which could become key under any future regulatory/legal requirements.
The Partners

IDnow is an identity verification platform provider with a vision to make the connected world a safer place. The IDnow platform provides a broad portfolio of identity verification solutions optimized for user conversion rates and security.

wait.id is a leading provider of open-source decentralized identity and wallet infrastructure already used by thousands of developers as well as governments, public authorities, DAOs, and businesses across industries.

Bloom is an all-in-one wallet for the IOTA, Shimmer, and EVM ecosystem. In this project, the identity token is stored in the Bloom wallet, enabling the user to prove their identity in the Web3 ecosystem.

HAVN specializes in the integration of hybrid blockchain technologies. It offers enterprise-ready blockchain infrastructure, data management, and Web3 tools as a service through its managed SaaS platform.

IOTA is a global non-profit that develops decentralized technologies for a new digital economy in a connected world. It redesigns the way people and devices connect to share information and value, removing middlemen.
Web3 KYC Evolution

In an era where data privacy and regulatory compliance are paramount, this groundbreaking KYC solution for Web3 respects individual autonomy and privacy. By tokenizing the identification process, users will be able to confidently engage with Web3 applications, knowing their personal information remains secure and off-chain.

As the regulatory landscape evolves, solutions like this will play a pivotal role in ensuring that DeFi and Web3 applications meet KYC compliance standards. To dive deeper into the IOTA Foundation’s work on user authentication and Digital Identities, please see the IOTA Identity Framework.
About Us

Founded in 2015, IOTA is a public goods infrastructure to bring trust in our digital world. Through IOTA, governments, organizations and people are able to interact with each other in a secure, trusted and verifiable way.

IOTA is one of the most established blockchain projects in the world and is primarily driven by a global ecosystem of non-profit organizations.

www.iota.org
info@iota.org