Tender KYC/AML Compliance and Privacy Design

Version A5 February 2020

Contents

1 Introduction

This document describes the design of the KYC/AML regulatory compliance and privacy policy implementations for transactions on the Tender platform being developed by Pacio.

Transactions for Tender is a broad term covering money (fiat or crypto) transfers, tokenised asset transfers, accounting/business transactions, or any transaction involving one or more usually two parties. In this document “asset” covers anything being transferred or involved in a transaction.

Tender aims to support the most popular real-world patterns, providing scalable, free and private asset transport and tools for compliance and privacy as required for particular apps and/or economies, leaving the choices to users (app developers) and regulators.

The proposed design supports any restriction or rule required by GDPR/FATF either now or as changed in the future, efficiently and flexibility.

For example, user private data could be kept in just one place, a Tender personal data app. All other apps and services could request user data from this app using security tokens received along with user transactions. Such a system would be suitable for typical questions organisations ask like "is the person older than 18?".

Users would only need to edit, allow access, or restrict access to their data in one place. This would be far more secure, convenient, and permit better GDPR compliance, than current practice where personal data ends up being copied and stored by multiple sites or apps. By restricting access to their data held in only one place, people could immediately reclaim their privacy – totally – whereas this is virtually impossible with current methods, since data stored by different sites and apps is no longer under the control of its owner – it has escaped forever. The probability of a leak also increases with every copy.

Access is layered (one doesn't have to know more than is needed) and anonymized in most cases. The flexibility allows currency or asset owner to meet new regulations that might arise, or impose restrictions, even ones similar to US sanctions with USD use and more...

At the same time, the platform could support non-complying economies with physical separation e.g. EU nodes not to store ISIS transactions.

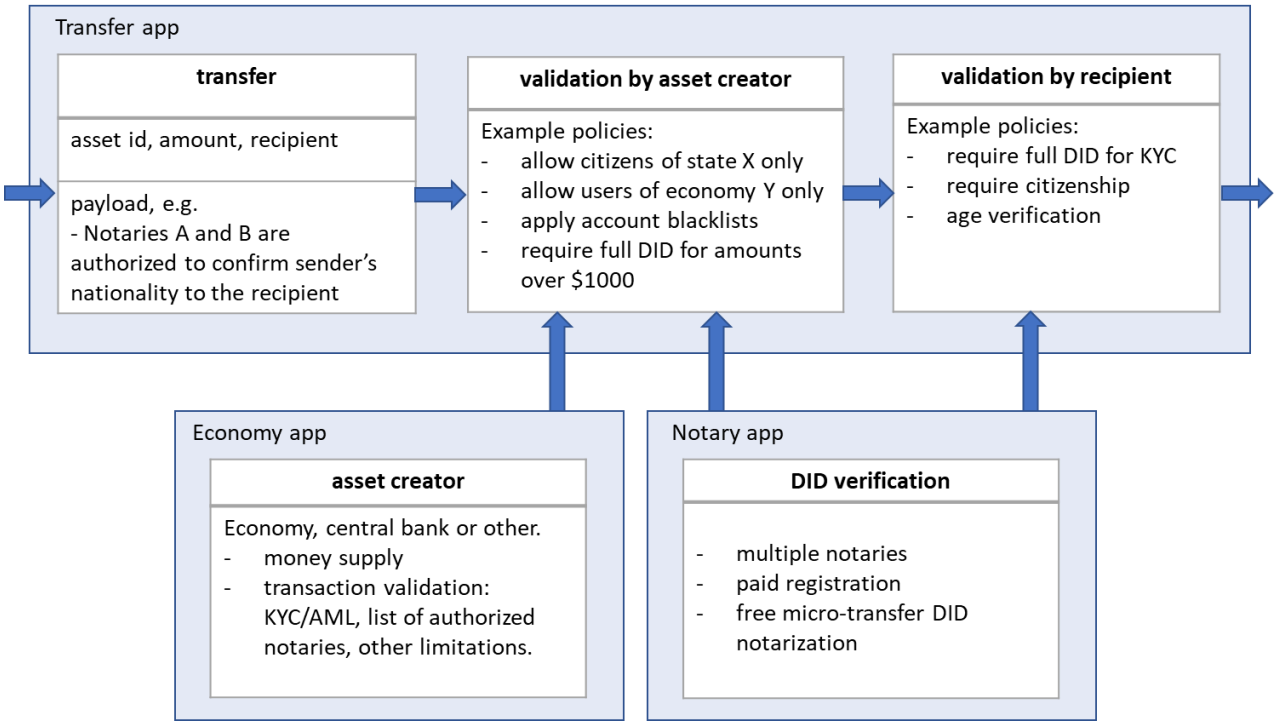
2 KYC/AML Policies

2.1 Overview

Tender transactions are designed to support most contemporary regulation policies:

- Transaction asset id can trigger validation with asset creator policies if defined.
- Recipient can define filters which incoming transfers need to pass to comply with regulations.
- Sender can attach required information to transactions.

Three apps are involved, the Transfer app, an Economy app, and a Notary app, which work together to handle transfers with flexible KYC/AML policy processing:



2.2 Implementation

The Tender platform supports multiple economies or markets via a constellation of apps for each economy and its ideology, covering transfers, currencies, funding, and whatever else apps may need. Whenever an app bridges (Holochain term) to a Tender app it joins the economy and can use its services. All apps have equal rights. Bridging to a Tender app will be relatively straightforward for Holochain apps, but also possible for other apps given demand and the development of appropriate interfacing and load balancing.

2.2.1 Transfer app

The Transfer app is a free common platform serving different economies and notaries. Assets can be free or regulated. Storage and validation resources of a node on Tender network are used in a fair manner: only the economies and notaries used by the node are served. User will have to explicitly

install the corresponding apps. In case an illegal entity creates its own asset, law-abiding nodes will never have to serve illegal transactions while running the same platform. If a new crypto-kitties app should load the network with billions tps, users not involved in the game will not have to share the load.

2.2.2 Economy app

The app implements basic meritocratic governance blocks for managing an economy: creating assets, defining monetary policies, etc.

The case of stable coins

Some central banks will eventually require full control of their currency replicas. Tender supports such transitions since it aims at providing compliant and free scalable micro-transfers. If central banks take care of their stable coin non-volatility, exercising all of its administration privileges, users of the platform will benefit.

2.2.3 Notary app

There may be different approaches. It would make sense to adopt conventional procedures into Tender rather than inventing something new for the MVP.

The flow.
Onetime identity verification:

- Users scan required documents and store them encrypted in their private chain on their devices.
- Users temporarily grant document read access to the verifier. The service is paid by the user or by a third party (bank, exchange etc.) as it is often the case now.
- Verifier creates an identity profile, stores and signs it on the DHT in an encrypted form.
- In case a legislation requires customer data to be verifiable by regulator later, encrypted document scans can also be stored/archived outside client devices (TBD).

KYC confirmations:

- On KYC requests tender wallet automatically issues an access token specifying the kind of identity information to disclose to recipient and attaches the token in transaction payload, e.g. “disclose my nationality to X”.
- Recipient uses the token and his private key to find and decode the confirmation, checks the auditor signatures and decides whether to accept the transaction.

Confirmations are free (served by the platform) and can be used for microtransactions. Tender application is simple. More demanding blocks are:

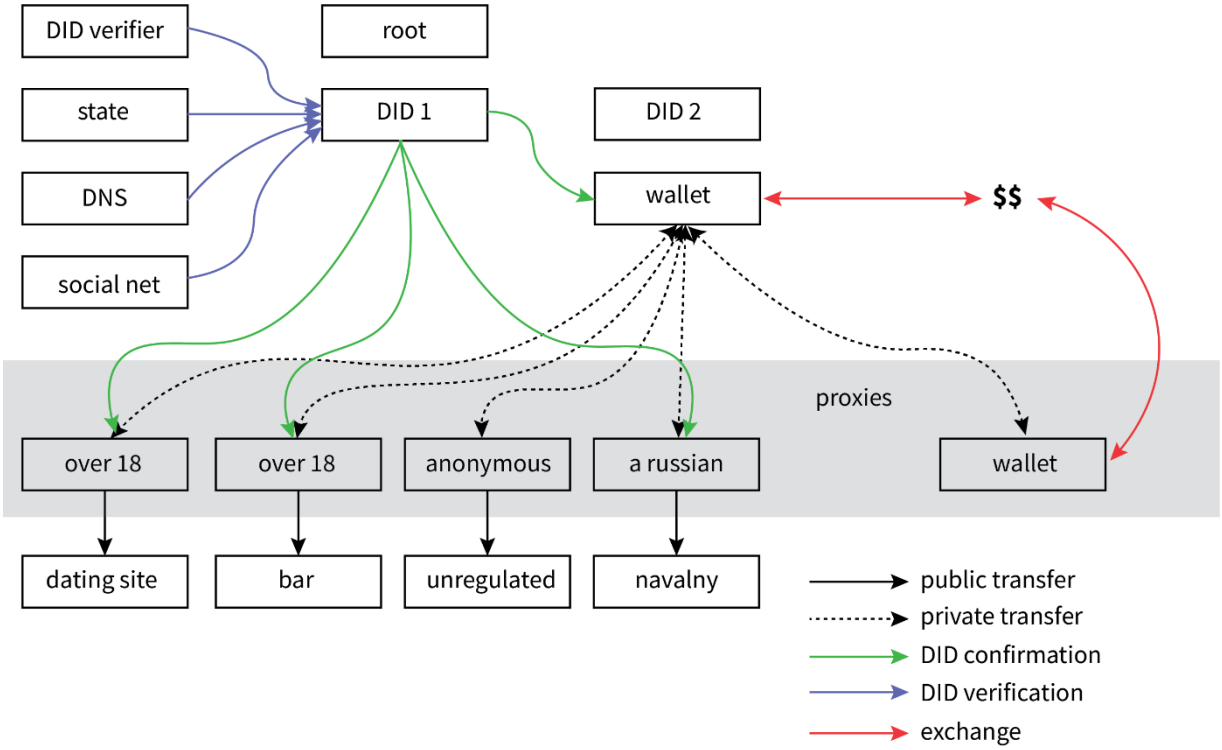
1. mobile app to help users make quality photos of their documents and tamper-proof videos where they show their passports;
2. pattern recognition software to automate verification;
3. access to id databases.

However, there are multiple agencies that already have these blocks implemented. And the market is highly competitive. The shortest way to have KYC support at tender rollout would be to invite an existing agency, have them provide the blocks and plug them into tender. Increase their business, share profits, provide tender grant to onboard the first 100K users to KYC free of charge?

We could define an open tender KYC API (to specify universal requests and access token format), build the first app in cooperation with an agency and invite other agencies to join, forking the open source app.

Or we can consider building a universal app where some of the blocks can be reused by multiple agencies: they register as verifier, use the scan/recognition infrastructure, receive requests, process them using their databases and sign. (ID can be verified and signed by multiple agencies.)

3 Digital Identities



3.1 Overview

Accounts

User creates the root account. It is saved and secured in a simple, transparent and decentralized way (like the guardian model in https://www.argent.xyz/security/). To prevent transaction history monitoring by third-parties, a proxy account is automatically created by default for each counter party. Transactions between the main account and proxies are obfuscated.

DIDs

User creates one or more identities:

- fills out forms and scans ID documents to be encrypted and stored *locally* in "paranoid" mode or replicated with guardians (friends) by default.

- user requests/buys verifications to have the ID signed. Whenever a new type of verification is needed it can be acquired/added/updated. User pays once (if needed), while all checks are free (served by the user node or tender “common good” model).

- when user needs a KYC confirmation for one of his proxy accounts, the app provides it to the requesting party via an end-to-end encrypted secure channel, disclosing just the minimum info to comply, from "the owner of the account is over 18" to a view token for the whole set of scans, forms and signatures.

Proxies

Proxies are accounts that serve as galvanic isolation for transaction history. They are created by default for each counter party and can be anonymous or individually connected to one of the user IDs or their parts. Proxies support KYC/AML requirements: although transfers from the main account are not traceable by third-parties, the owner of the accounts can choose to disclose origin of funds and prove ownership of the identity.

Privacy

- Proxy accounts replicate the real-world model, where user discloses part of his identity to each counter party without sharing transaction history with others.

- Third-party data miners cannot see connection between proxy and main accounts.

KYC/AML

- If an app implements a KYC/AML policy, it can request user to disclose either identity or origin of funds or both. Private transfers contain encrypted payload which can be decrypted by the owner (both sender and recipient) to disclose it upon an AML request.

- If regulator requires apps to store client ID info, tender wallet can be configured to save it. GDPR permission removal can also be automated.

3.2 Implementation

The functions can be packaged into a tender DID app and controlled from wallets. Holochain's personas can be used as a base.