PRIVATE: a framework for Privacy Preservation through Resolution of Identity via Verification and Attestation for Travel Rule CompliancE

v 0.2

March 21, 2022

Authors:

Francesco Piccoli, AnChain.AI, francesco.piccoli@anchain.ai

Vadim Slavin, GlobaliD, vadim@global.id

Summary

We present a framework for enabling enhanced due diligence of non-custodial wallet addresses involved in an virtual asset transfer with a compliant Virtual Asset Service Provider (VASP) subject to the Travel Rule requirement.

PRIVATE framework enables the obliged entity to verify counterparty non-custodial wallet information provided by the known (KYC'd) participant of the transaction (originator or beneficiary). At the same time, it allows for maximum privacy protection of personal information of the wallet owners.

The framework provides tools for full compliance with the Travel Rule enabling due diligence of non-custodial wallets beyond current expectations of the Financial Action Task Force (FATF).

This paper outlines an additional set of tools for scoring risk of virtual asset transactions making the distributed finance (DeFi) and non-fungible token (NFT) ecosystems safer for all parties involved.

Introduction

On March 15, 2019 at a Blockchain Symposium, FinCEN's Director Kenneth A. Blanco made an announcement on the Travel Rule: "It applies to CVC (Convertible Virtual Currency) and we expect you to comply, period". Mr. Blanco's comments followed FinCEN's release, in May 2019, of its long-awaited guidance on the application of existing Anti-Money Laundering ("AML") rules, including the Travel Rule, to virtual currency businesses.

Further, during its June 2019 plenary, the Financial Action Task Force ("FATF"), the G20's financial crimes watchdog, issued Recommendation 16 requiring Virtual Asset Service Providers **("VASPs")** to share Personal Identifiable Information ("**PII**") and Know-your-customer **("KYC")** data between transacting sender and receiver users before executing the transaction over EUR/USD 1000. VASPs include Cryptocurrency Exchanges, Bitcoin ATMs and Custody Providers, among others.[ref]

Several competing frameworks have been proposed to enable two obliged VASPs to exchange information about a virtual asset transaction. These require collaboration and communication between the two VASPs.

On October 28, 2021 FATF released updated recommendations touching DeFi, NFTs, stablecoins, and wire transfers. In particular, section 179(c) updates the guidance to include non-custodial wallets [ref]. There FATF acknowledges that special challenges exist in complying with the Travel Rule requirements when dealing with non-custodial wallets. The privacy preservation and self-sovereign nature of identities of owners of non-custodial crypto addresses makes it especially challenging for VASPs to comply with the Travel Rule's identity requirements and perform risk analysis for each transaction to and from such wallets.

In this paper, we present PRIVATE, the framework for Privacy Preservation through Resolution of Identity via Verification and Attestation for Travel Rule Compliance. PRIVATE enables enhanced due diligence of the party represented by a non-custodial wallet. Relying on this framework enables VASPs to go above and beyond expected practice for compliance with the latest FATF recommendations for the Travel Rule and to do so while preserving the privacy of owners of non-custodial wallets (NCWs).

While today FATF expects only the identification of owners of NCW to be possible, PRIVATE enables the actual verification of this information. This ability presents additional tools for AML regulators and industry participants to strengthen the security of distributed financial systems.

Table of Contents

Summary 1

Introduction 2

Table of Contents 4

Glossary 5

Requirements 6

- Travel Rule for asset transfer to/from NCWs 6
- Risk assessment 8
- Identification 9
- Verification 9
- Trust 10
- Privacy preservation 10

Current approaches 11

- Pending challenges 12

Proposed solution 13

- End-to-end solution for Travel Rule compliance 13
- Identity attestation 14
- Data matching for attestation 19
- Ownership Credentials 20
- Authorized access to the attestation APIs 23
- Communication protocol 24

Benefits of PRIVATE (Summary) 25

References 27

Appendix 28

- GlobaliD 28
- AnChain.AI 29

1. Glossary

NCW - Non-Custodial Wallet, or unhosted wallet, are wallets that are not hosted by a third-party Custodian but are directly controlled by an individual without the need for an intermediary.

VA - Virtual Asset, a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. [ref]

VASP - Virtual Asset Service Provider.

O - Originator (sender), the person or legal entity originating a transaction.

B - Beneficiary (recipient, receiver), the person or legal entity on the receiving end of the transaction.

Ao - crypto address of the Originator involved in the transaction.

Ab - crypto address of the Beneficiary involved in the transaction.

Co - Custodian of the crypto address (VASP) involved in the transaction belonging to the Originator (sender).

Cb - Custodian of the crypto address (VASP) involved in the transaction belonging to the Beneficiary (recipient).

OFAC - The Office of Foreign Assets Control of the US Department of the Treasury which administers and enforces economic and trade sanctions based on US foreign policy and national security goals.

KYW - Know Your Wallet process which checks whether the given address is on the OFAC sanctions list, whether it belongs to a known entity, and the subjective risk score associated with the address.

CDD - Customer Due Diligence.

2. Requirements

Per Travel Rule compliance requirements, KYC of the Originator **(O)** and the Beneficiary **(B)** must be known to both the beneficiary institution and the originator institution. This whitepaper focuses on institutions that are Virtual Asset Service Providers (VASPs) who interact with Non-Custodial Wallets (NCWs).

2.1. Travel Rule for asset transfer to/from NCWs

The latest guidance from FATF clarified their recommendations for financial activities involving Virtual Assets (VAs). More specifically, FATF reiterated the recommended obligation to obtain, hold, and submit required originator and beneficiary information associated with virtual asset transfers in order to facilitate the identification and reporting of suspicious transactions [ref, sec 183]. Here is the summary of the recommendations.

Data item and required action	**Originator VASP**	**Beneficiary VASP**
Originator Information	Requirement to submit the necessary data to a beneficiary VASP is mandatory. VASP needs to verify the accuracy as part of its CDD process.	Beneficiary VASP needs to obtain the necessary data from ordering VASP. Data accuracy is not required. The beneficiary VASP may assume that the data has been verified by the ordering VASP.
Beneficiary Information	Required to submit the necessary data to the beneficiary VASP. Data accuracy is not required, but the ordering VASP must monitor to confirm no suspicions arise.	Required to obtain the necessary data from the ordering VASP. The beneficiary VASP must have verified the necessary data and needs to confirm if the received data is consistent.
Actions required	(1) Obtain the necessary information from the originator and retain a record. (2) Screen to confirm that the beneficiary is not a sanctioned name.	(1) Obtain the necessary information from the ordering VASP and retain a record. (2) Screen to confirm that the originator is not a sanctioned name.

Originator/beneficiary information in this case is referring to [ref, section 182c and 183c]

- name,
- physical (geographical) address, OR
- national identity number, OR
- customer identification number (i.e., not a transaction number) that uniquely identifies the originator/beneficiary to the ordering institution, OR
- date and place of birth;

FATF guidance ([ref, sec 295]) also considers virtual asset transfers to and from non-custodial (or unhosted) wallets.

While the ability of obligated entities to check the accuracy of information about the owner of a non-custodial wallet is not anticipated by FATF, PRIVATE establishes a framework where such check of accuracy is possible. This framework enables VASPs to perform enhanced due diligence on the owner of the non-custodial or un-hosted wallet address involved in a transaction.

Here is one possible sequence of obligated entity control activities as recommended by FATF:

Outbound transaction (Originator VASP sending assets to a NCW)

1. Collect the destination wallet address and the KYC of the Beneficiary from the Originator who is a customer of this VASP; e.g. “Please fill out this form to provide information about the intended recipient of this transaction. If you are withdrawing the funds to your own non-custodial account, please provide proof of your ownership of this beneficiary address.”

2. Verify that the Beneficiary’s KYC matches the true owner of the provided destination address

3. Check beneficiary information and their address against a sanctions database (perform “the OFAC check”)

4. Score the risk of sending funds to the given NCW address by performing enhanced due diligence on the transaction

5. Determine if the transaction should be allowed based on the risk score

6. Store information for the transaction as mandated by the Travel Rule without transferring it anywhere

Inbound transaction (Beneficiary VASP receiving assets from a NCW)

1. Request KYC of the Originator from the Beneficiary (the customer of this VASP): e.g. “We received a request to transfer funds to your account. To release the funds, please fill out this form to provide information about the sender. If you are sending these funds to yourself, please provide proof of your ownership of the address from which the funds were sent.”
2. Verify that the Originator’s KYC matches the true owner of the provided originator address
3. Check Originator KYC and and their address against a sanctions database (perform “the OFAC check”)
4. Score the risk of receiving funds from the given NCW address by performing enhanced due diligence on the transaction
5. Determine if the received funds should be released to the Beneficiary based on the risk score
6. Store information for the transaction as mandated by the Travel rule without transferring it anywhere

2.2. Risk assessment

Per FATF recommendations, in order to approve the transaction, the VASP must implement enhanced due diligence processes to evaluate whether a transaction should be allowed. There are two separate checks: sanctions screening and transaction risk assessment.

Sanctions screening requires clearing the NCW address, its owner, and the VASP’s customer against the sanctions list. The VASP already must collect and verify KYC for

every one of its customers. The only remaining check is for the owner of the NCW address.

Transaction risk assessment is based on the risk-management process implemented by the VASP. It can include many factors. For example, the NCW address can be evaluated based on its age, prior activity, balance history, association with other known red-flagged addresses, etc. There are several reputable services specializing in providing such risk scores. Additional scoring tactics can also be used. For example, if the owner's address is provided incorrectly on several occasions or a different owner is reported by the VASP's customer each time, the risk score for this address can be amended accordingly.

An obliged organization must take this risk assessment into account to determine whether to authorize the transaction or not. This is the expected risk management process to be performed for both incoming and outgoing transactions in order to limit money laundering and the financing of illicit services.

2.3. Identification

One of the most important requirements of the Travel Rule is identification of the parties involved in the transaction. Identification involves collecting personal, identifiable information to the highest level of assurance possible. For a compliant VASP, identification of their customer is already performed by the time the first transaction is created. On the other end of the transaction, the Travel Rule requires information be collected about the other, unobliged party, i.e. the owner of the NCW. The Travel Rule directs the obliged party to request this information directly from the originator as a condition for initiating or approving the transaction or determining that the same person is the owner of wallet addresses on both sides of the transaction.

2.4. Verification

While the accuracy of collected personal information about the other party is not expected by FATF ([ref, section 182c and 183c]), the verification of this information should be performed if such a solution is indeed available. Doing so is good risk management practice. Such verification can greatly enhance the security of each transaction and help score the risk of each transaction in order to reduce the threat of money laundering and other illicit financial activities.

Enhanced due diligence on the other party in control of the NCW should include attestation of owner's information as reported by the VASP customer. This information should be attested by reliable, independent sources which can provide sufficient proof of both ownership and personal information belonging to the owner of the NCW.

2.5. Trust

Any organization that is allowed access to PRIVATE must have a legitimate purpose. A reputable VASP implementing enhanced due diligence or financial crime investigators must be registered with relevant authorities in order to have access to such a sensitive identity verification service.

Also, the source of attestation must also be trusted to report information accurately.

2.6. Privacy preservation

The KYC information of the owner of each NCW address, if available for attestation, must be protected. The privacy of the true owner of the NCW must be preserved in case the information available for attestation is not itself accurate. No information can ever be retrieved outside of the intended use case of verification of known identity and wallet ownership. The threat of information leakage must be minimized if not eliminated altogether. Only then may consumers be willing to provide their information at scale to make the platform useful and sustainable.

Such assurances must be given by the technical architecture of the solution and not be subject to organizational policies or legal jurisdictions. In fact, the solution must make it impossible for law enforcement to compel any person or entity to provide access to services beyond what was originally intended.

3. Current approaches

Since the Travel Rule recommendation was introduced for VASPs in 2019, multiple organizations have worked together to provide technical standards to the industry. Following is a list of some of the major contributors:

OpenVasp: open protocol among VASPs for mutual exchange of originator and beneficiary information. It takes a decentralized and privacy-preserving approach by leveraging the Ethereum blockchain for the authentication and exchange of information. It deploys a standardized smart contract on the Ethereum blockchain which represents a VASP identity on the blockchain, and it associates a code and account number to each VASP. Messaging protocol-agnostic, the Ethereum Whisper protocol is the suggested messaging protocol highlighted in the whitepaper. [ref]

InterVASP: The Joint Working Group on interVASP Messaging Standards (JWG) comprising over 130 technical experts from around the world, developed interVASP Messaging Standard IVMS-101, a universal common language for communication of required originator and beneficiary information between VASPs. It provides a standard data model for use in transmitting required originator and beneficiary information. [ref]

TRISA: The Travel Rule Information Sharing Architecture is a peer-to-peer mechanism for VASPs to comply with the respective Funds Travel Rule for transaction identification exchange between originators and beneficiaries. TRISA created a Global Directory of VASPs and an open-source architecture for the sharing of information between VASPs. [ref]

TRP: The Travel Rule Protocol Working Group is a global independent industry body. They created an open-source API that uses the IVMS-101 data model standard for the transmission of required information. [ref]

TRUST: The Travel Rule Universal Solution Technology (TRUST) is a protocol designed for VASPs to comply with the Travel Rule requirements while protecting the privacy of their customers. Several US-based VASPs and financial institutions are currently members of the TRUST consortium, but an end-to-end solution still has not been developed (at the time of writing of this paper). The protocol is designed to avoid a central storage of customer data, it comes with a proof of address ownership mechanism, and can only be joined by members who meet certain anti-money laundering, security, and privacy requirements. [ref]

3.1. Pending challenges

Although the above-mentioned protocols provided comprehensive technical standards for the industry, the evolving nature of the VA industry required the introduction of new recommendations from FATF. Recommendation 179(c), published on October 28th 2021, extends the Travel Rule requirements to non-custodial wallets, bringing new technical challenges for VASPs to remain compliant.

By definition, non-custodial wallets are not hosted by a third-party Custodian, but they are directly controlled by an individual without the need for an intermediary. This means there is no obliged entity which can be held accountable to provide identification of the owner of the wallet. This is why Travel Rule compliance expected by FATF only requires the collection of identity data from either the Originator or Beneficiary serviced by the obliged VASP and not both. Such an approach weakens regulators' ability to ensure the

security of the financial system as well as to prevent money laundering and fianancing of terrorist activities.

4. Proposed solution

We propose to establish a privacy preserving framework for complying with the Travel Rule for VASPs dealing with non custodial wallets (“**NCW**”). Traditional approaches to KYC are privacy shredding. This means the privacy of owners of NCWs cannot be guaranteed. We propose a radically different approach to enable compliance while preserving the privacy of owners of the NCWs.

This framework enables authorized entities to request attestation of identity information disclosed to them by their customer, the Originator or the Beneficiary of a transaction. Under PRIVATE, authorized entities can determine whether provided information verifies NCW owner identity; in doing so, authorized entities perform enhanced due diligence on the transaction and minimize potential money laundering activities. Attesting known information is the only service possible using this framework. The architecture of the framework makes it impossible to reveal the identity of the owner if that information is not available a-priori.

4.1. End-to-end solution for Travel Rule compliance

There are two use cases which require Travel Rule compliance where a non-custodial wallet is involved. A non-custodial wallet either serves as the Originator of a transaction with an obliged entity or a non-custodial wallet serves as the Beneficiary of an obliged entity’s ordering transaction.

Consider the following use case. A customer of a VASP (Originator) initiates a transaction to move virtual assets to a specific address. The VASP determines that this address is not in its custody and collects information from the Originator about the

Beneficiary, the owner of the address where the assets are intended to be transfered. The Originator must provide this Beneficiary information as a prerequisite for a successful transaction. The VASP uses a 3d party service to look up the presumed custodian of the Beneficiary’s address. However, what if the Beneficiary's address is un-hosted and there is no custodial entity that can provide this information?

Consider the alternative use case: a non-custodial wallet owner initiates a transaction. In this case, the Beneficiary is a customer of a VASP which must comply with the Travel Rule. The VASP is now responsible for determining whether funds should indeed be released to the Beneficiary. The VASP can collect information about the Originator from the Beneficiary and attest that it correctly identifies the owner of the Originator address. Based on the results of this attestation, the VASP must decide whether to allow this transaction or freeze and report the Beneficiary’s account for further investigation.

In both cases above, the Originator and Beneficiary can indeed be the same person and the transactions can be treated as a funds transfer (withdrawing or adding funds) rather than a payment. In this case, the person must show proof of ownership of their non-custodial account.

4.2. Identity attestation

For simplicity, consider a use case where the Originator is transferring funds to a non-custodial wallet via their custodian VASP. They cannot provide their own proof of ownership which means their custodian VASP should treat this as funds transfer, not a withdrawal. Incoming funds transfer use case is treated the same way with respect to how identity attestation is performed.

Compliance with the travel rule requires identification of the external party in a transaction. A VASP can collect this information from its customers. Furthermore, it can check with an external service to attest that collected information is accurate.

Consider a service, let's call it "**Data Warehouse**", which exposes a simple API endpoint as follows:

DataWarehouse.attestOwner ("Owner Attestation API")

This API endpoint is exposed by the Data Warehouse service provider and takes in a wallet address and KYC information of the reported owner for attestation. It responds with the information whether a match was found, what level of assurance the original owner information was verified to and a risk score for the wallet address itself.

Parameters

Name	In	Type	Required	Description
address	path	string	true	Public NCW address on a specific ledger
ledger	path	string	true	The name of the ledger: e.g. "BTC", "ETH", …
kyc	path	object	true	KYC information as an object which contains such attributes as "name", "date of birth", etc.

Response Schema

Status Code **200**

Name	Type	Required	Description
match	string	true	Yes, KYC information provided matches the information of the owner of the provided address No, information provided does not match the information of the owner of this address Inconclusive, no owner information is available for the provided address
level	string	false	If **match** is Yes or No, also return the level of identity assurance used to provide this response: e.g. "bronze", "silver", "gold". See below for more information.

riskScore	string	true	Risk score assessed by the Data Warehouse from other potential sources of information such as analysis of the blockchain transactions this address participated in. See below for more information.

Levels of identity assurance describe the level of certainty in the identity information available for attestation. We recognize three distinct levels of identity assurance:

- **Bronze**, information was self-declared by the owner of the address
- **Silver**, information was verified via a government ID with a biometric match
- **Gold**, information was verified using two independent silver-level verifications

The level of identity assurance with which the attestation is made is important because the VASP can assign different levels of risk to each level. For example, a response of

{ *"NO" (no match), "Bronze"* }

means that the owner's information was self reported when the address ownership verification was performed. If it was self-reported inaccurately, the *"NO" (no match)* result is not a strong indication of misrepresentation. If the owner's information available is at Silver level, the case for misrepresentation is stronger. This may mean that the Originator does not know the true owner of the Beneficiary, is trying to send funds to the wrong person by mistake, or has another malicious intent to hide the details of the transaction.

Even if the DataWarehouse.attestOwner **(**"Owner Attestation API") response is

{ *"Inconclusive" }*

the Risk Score factor may reveal that the address was not interacting with other high-risk addresses. Identity information can, of course, significantly lower the Risk Score calculated by a 3d party. However, the details of the implementation of enhanced due diligence is left to the discretion of each VASP taking advantage of this framework.

The Owner Attestation API endpoint must protect the privacy of the true owner of the non custodial address. Data Warehouse can only confirm, or attest, what is already known without revealing any additional information. No additional information is to be available to the Data Warehouse in the event its service is compromised. Here is how this can be implemented.

This Risk Score returned by the above API endpoint can measure multiple factors related to prior activity of this address, its interaction with other potentially sanctioned or fraudulent addresses, or any other activity that may indicate risk. The Risk Score can be provided by the same Data Warehouse or by another service altogether via a separate endpoint.

The availability of owner data for attestation is provided by another service, let's call it "**Verifier"**. This service performs verification of NCW address ownership and the identity information provided by the owner at whichever level available. This is accomplished by offering "**Address Ownership Credentials**" to individuals. As a result of this service, owner information is added to a vault. More on this in section 4.4.

To protect the privacy of individuals, the Data Warehouse must be allowed to access a third sub-service, let's call it " **The Vault**". The Vault is responsible for storing and securing encrypted information about the owners as provided by **Verifiers**. In its simplest form, the Vault contains a table with the following table schema (columns):

Record UUID:

A unique identifier of the record

Wallet address info:

The wallet address itself and which ledger (blockchain) it is on.

Encrypted identity information of the owner:

KYC information as required by the Travel Rule compliance

Identity assurance level of the owner's information:

A designation of the level of certainty that KYC information does belong to the owner of the address and was provided correctly and truthfully: Bronze, Silver, Gold

Date of creation:

The date the record was created

Verifier which added this record:

Which service provider verified ownership of address and checked the identity information of the owner.

There may exist more than one Record UUID for the same wallet address. Different Verifiers can add records for the same address and they can do it multiple times.

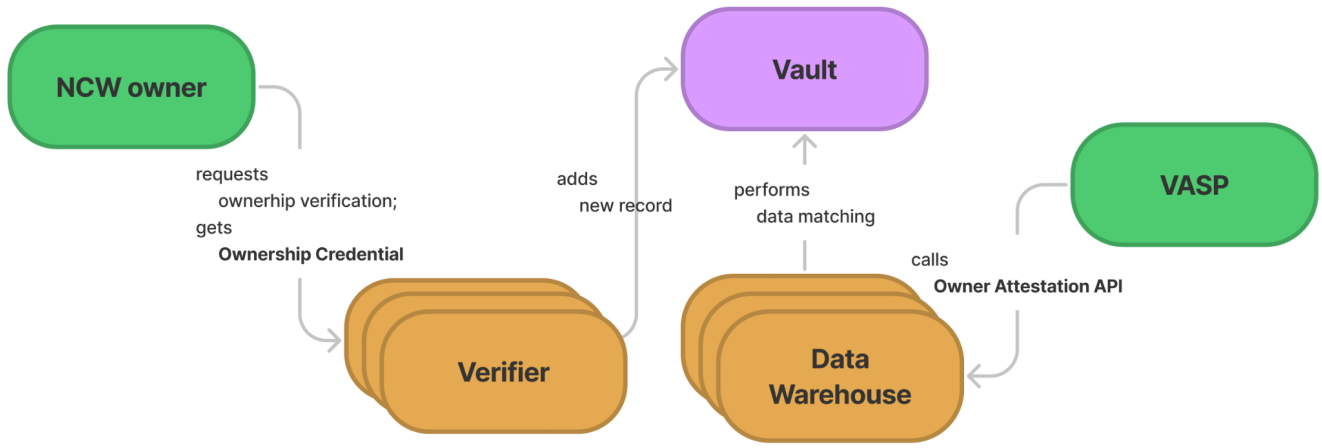

Diagram 1: Participants of the PRIVATE framework

The Data Warehouse does not need the key to decrypt the identity information stored in the Vault. The Vault exposes the matching function as an API endpoint available only to registered Data Warehouses. The Vault itself performs the data manipulation internally and provides the response to the Data Warehouse. If the Vault implements homomorphic encryption the data matching can be enabled without decrypting personal information stored [ref]. Otherwise, the matching can be performed inside a

trusted execution environment implemented by the Vault. [ref] Either way, the Data Warehouse does not have direct access to the personal data in the Vault.

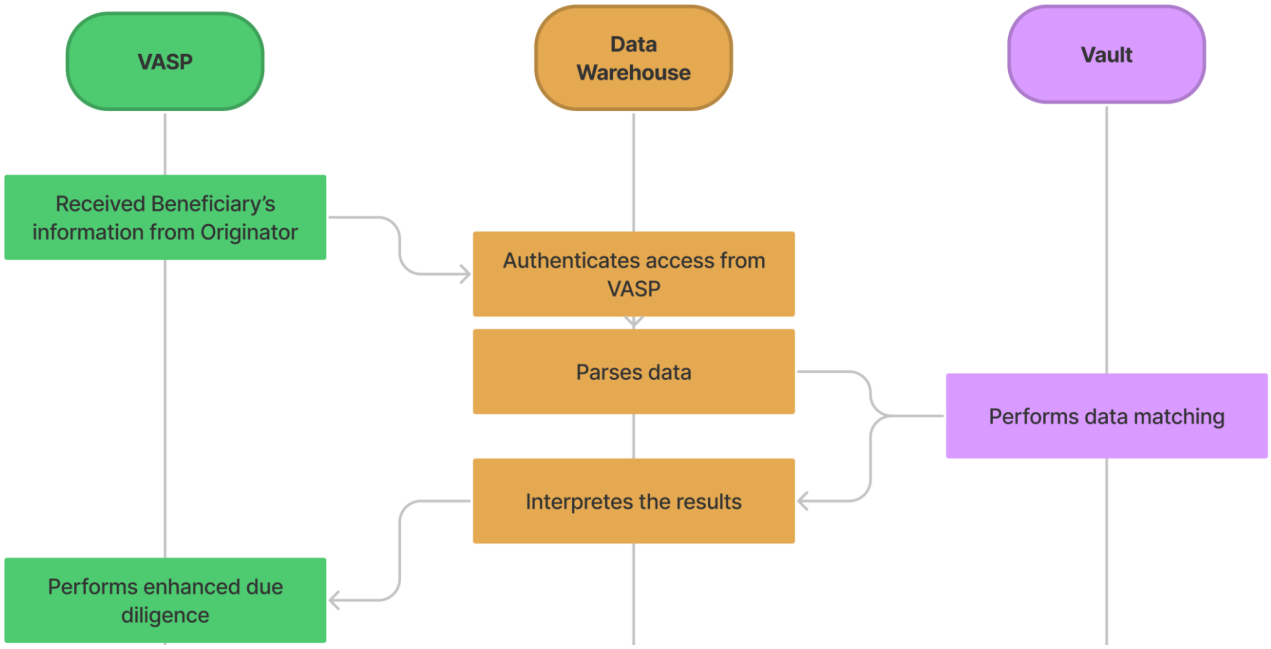

Diagram 2: sequence of events for verifying NCW owner's information

4.3. Data matching for attestation

To further protect security of stored personal information, service access and data matching are handled by two separate entities. The Data Warehouse can be considered a proxy for the data matching and encapsulates the attestation service. It implements business rules governing VASP's access to this service, billing, support, etc. It also defines the conditions under which a positive attestation is reported back. For example, it defines the thresholds for a fuzzy match which will determine whether a name such as "Tom Jones" is a match of "Tom A. Jones".

The Vault is the secure protector of private data. It is also a trusted entity which performs the data matching. The exact implementation of this service is left up to the industry and may include homomorphic encryption and/or a trusted execution environment.

Regardless of the specifics of the implementation the matching algorithm reports whether the results are MATCH or NO MATCH when the two string values are compared to each other. For example, as input, it may take the levenshtein distance [ref] of the two string values for the presumed and actual KYC information associated with the NCW address.

4.4. Ownership Credentials

One important part of the framework is how identity information is added to the Vault such that attestation is later possible.

The **Verifier** enables address ownership verification directly to the consumers. Upon successful verification of address ownership, Verifier issues one of three types of Ownership Credentials to the user depending on the level of assurance that the user provided their correct information:

- **Bronze Ownership Credential** requires
    - verified phone number and
    - self-declared identity information without formal verification: legal name, date of birth, home address
- **Silver Ownership Credential** requires
    - verified phone number and
    - identity information verified via a government ID or another source of such information, e.g. the financial institution of the person such as a bank

- **Gold Ownership Credential** requires two independent verifications of the same information. For example, a verification of a government ID or a utility bill which matches the information reported on this user by a financial institution such as a bank.

Here, as an example, we consider an implementation of a self-sovereign identity wallet, controlled by the owner, to which credentials can be added.

Each Ownership Credential has the same schema:

Attribute name	**Format**	**Notes**
wallet_address	string	The address for which the verification is made
wallet_ledger	string	The ledger of the address, e.g. “BTC” or “ETH”
owner_legal_given_name	string	First name of the owner
owner_legal_surname	string	Last name of the owner
owner_date_of_birth	yyyy-MM-dd	Date of birth in ISO 860 format [ref]
owner_phone_number	E.164	Phone number in E.164 format [ref]
owner_address_street_1	string	The first line of the street address
owner_address_street_2	string	The second line of the street address
owner_address_city	string	The locality of the address (e.g. city or town)
owner_address_province	string	The administrative region of the address (e.g. state or province)
owner_address_postal_code	string	The postal code of the address (e.g. zipcode)
owner_address_country	string	The country of the address

The schema ensures ease of data matching which can be accomplished by comparing each attribute separately. This enables matching of the address on country and city even if the street address was recorded in a different format.

Date of birth, while not being used directly for owner verification, will extend the applicability of these credentials to other use cases. This, in turn, will create more incentives for consumers to get such a credential. For example, a silver level credential may be used for a strong form of age verification for distributed apps running on the blockchain.

Upon successful issuance of one of the Ownership Credentials, the Verifier adds user's encrypted identity information to the Vault under a new Record UUID. This can happen more than once for the same wallet address if the user requests such verification several times. Data Warehouse does not have to guarantee that the information provided is the same every time. However, it can utilize a potential discrepancy to enable scoring of the risk profile of the address. To avoid such discrepancy the user must be encouraged (but not required) to provide verified information as opposed to self-declared information only.

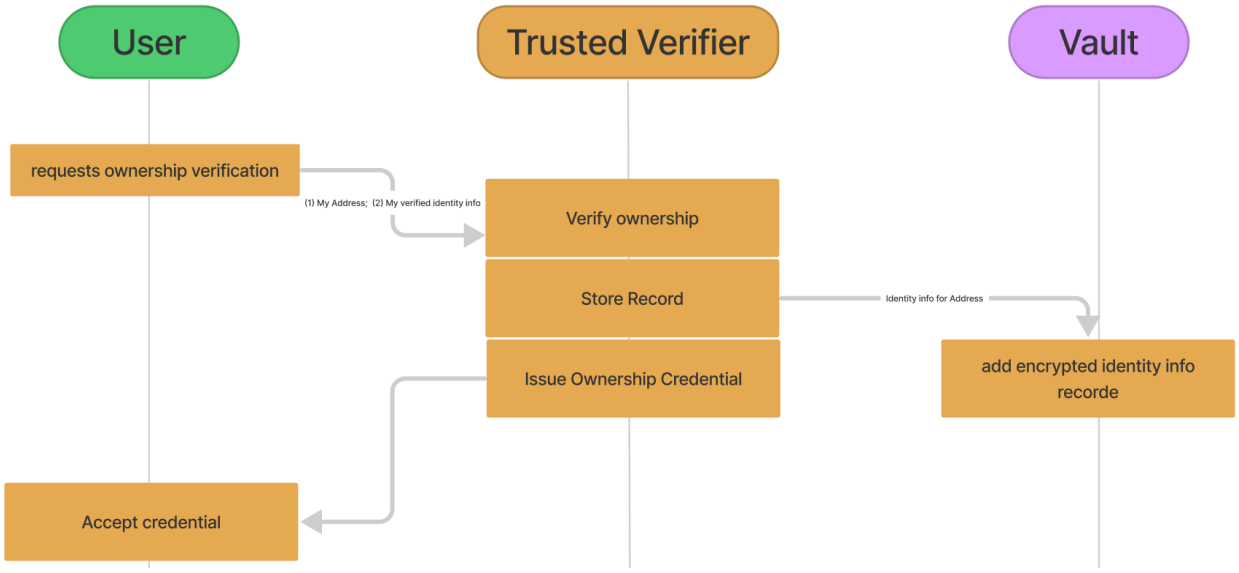

Diagram 3: Sequence of events for ownership verification

However, in the end, the user must decide the level of friction they prefer in exchange for the benefit provided by the Ownership Credential. These benefits can vary but must be valuable enough to encourage as many consumers as possible to obtain these credentials. Here are some of the potential benefits and use cases for the Ownership Credentials:

- A regulated, compliant VASP may request such credentials as a condition for withdrawal of funds to the user's non custodial wallet.
- A newly minted virtual asset or an NFT may choose a more equitable airdrop of funds to specific addresses such that the owner verifies ownership of that address first. This significantly reduces the threat of sybil attacks.
- A peer-to-peer marketplace can assign a higher level of reputation or authority to those members that have connected their non custodial address using a Silver or a Gold Ownership Credential.
- Higher level credentials may reduce the cost of transaction in decentralized ecosystems because they represent lower risk associated with the transaction. One such example was proposed by the tbDEX protocol. [ref]
- Other use cases may come up as the ownership credential service becomes readily available.

All of the above use cases, as well as the ability to obtain the Ownership Credentials themselves, are made possible via a growing number of digital identity wallets available on the market today.

4.5. Authorized access to the attestation APIs

Once an identity has been added to the Vault and an Ownership Credential has been issued, VASPs need to be able to use this information. As mentioned above, the Data

Warehouse exposes a simple API endpoint (the “Owner Attestation API”) that takes as parameter the address and KYC information provided by the VASP’s customer and performs an identity attestation against the information stored in the Vault.

VASPs would need to coordinate with the Data Warehouse to obtain permissioned/trusted access to the API. One easy way of implementing this would be for the Data Warehouse to issue a client key to the VASP, but each Data Warehouse may independently decide how to handle the access control.

Rate limitations should be applied to services like this to prevent abuses by rogue agents with access to these services.

4.6. Communication protocol

There are two scenarios under the Travel Rule requirements where exchange of information is needed:

- Virtual asset (VA) is transferred from VASP to VASP
- Virtual asset (VA) is transferred from VASP to NCW or from NCW to VASP

While the first scenario has been carefully addressed by some of the organizations mentioned above, PRIVATE framework addresses the second scenario.

The two scenarios differ substantially. There are no requirements for NCW owners to obtain, send, or store the information mentioned in the FATF guidelines. Therefore, the communication protocols outlined by some of the existing frameworks are not necessarily applicable when NCWs are a part of the equation. There is no other party with which to establish a secure communication.

A secure and privacy-oriented connection needs to be established between the owner of a NCW and the provider of the end-to-end solution (Data Warehouse, Verifier, and Vault),

and from a VASP and the same provider. The communication can be asynchronous, but it needs to ensure a near-real time response time to the VASP so as to not disrupt any of its business operations.

For the sake of brevity, this whitepaper will not enter into the details of how to implement such a secure connection. It is left to the discretion of the implementers of such end-to-end solution.

Under PRIVATE, the privacy of the true owner of the non-custodial address is always protected, as the Data Warehouse can only confirm, or attest, what is already known by the VASP without revealing any additional information. The introduction of the Vault sub-service storing and securing encrypted information about the owner of a NCW ensures that no additional information is made available to the Data Warehouse in the event its service is compromised. On the other hand, no information about the VASP customer is shared with the owner of the NCW participating in the transaction.

5. Benefits of PRIVATE (Summary)

The primary focus of this framework is to enable stronger, more convenient compliance with Travel Rule compliance requirements without compromising the security and privacy of the consumers within the DeFi and NFT ecosystems. It strives to find the right balance between privacy preservation and regulatory compliance.

Privacy preservation of this framework must be underscored. The architecture of the framework prevents leakage of sensitive private data even in the case of unauthorized access. Only brute force, repeated verification requests can attempt to reveal the true identity of an address owner by guessing the name each time. Trivial API access limits can address this threat.

Enabling verifications of ownership of non-custodial wallet addresses enables a number of other use cases:

- Proving the reason for withdrawing funds from a centralized exchange
- Attaching non-custodial address to a digital, pseudo-anonymous identity which enables multi-factor authentication and liveness verification to prevent spam

These services can be equally valuable to enablers of the transactions, the VASPs, and law enforcement and financial crime investigators.

Coupling verification of ownership with identity information at various levels of assurance also enables “Greening” of the ledgers. Greening refers to grouping all created addressed on a ledger into three lists:

- **Red list** which contains all known malicious addresses implicated in illicit activity or otherwise flagged by risk detection algorithms;
- **Gray list** which contains all addresses lacking any useful information about them, e.g. dormant addresses;
- **Green list** which contains addresses with identity information attached to them.

Consider the following table.

	Gray	Green	Red
Owner unknown	Every freshly created address starts here	-n/a-	Bad addresses flagged
Owner known	-n/a-	Every address should be here	Law enforcement can get involved

The process of “Greening” is therefore converting as many addresses on a ledger from the gray list (or even red list) to the green list.

While PRIVATE aims at supplying VASPs with the right tools to fully comply and go beyond FATF recommendations, we invite industry participants, law enforcement, and regulators to provide feedback on the framework outlined in this whitepaper. We also encourage companies who want to build an end-to-end solution (or parts of it) based on this framework, or use one of the existing ones, to reach out to our team at info@anchain.ai and info@global.id.

6. References

- “The ‘Travel Rule’ - Can Cryptocurrency Comply?” Sia Partners - Global Management Firm, https://www.sia-partners.com/en/news-and-publications/from-our-experts/travel-rule-can-cryptocurrency-comply.
- Updated Guidance for a Risk-Based Approach - Fatf-Gafi.org. https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
- Riegelnig, “OpenVASP: An Open Protocol to Implement FATF’s Travel Rule for Virtual Assets,” Nov 2019. https://www.openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf
- Joint Working Group on interVASP Messaging Standards, “interVASP Messaging Standards,” https://intervasp.org/wp-content/uploads/2020/05/IVMS101-interVASP-data-model-standard-issue-1-FINAL.pdf

- “Whitepaper Version 8.” *Trisa.io*, 6 Apr. 2021, https://trisa.io/trisa-whitepaper/.
- TRP, https://www.travelruleprotocol.org/
- “Homomorphic Encryption.” *Wikipedia*, Wikimedia Foundation, 18 Nov. 2021, https://en.wikipedia.org/wiki/Homomorphic_encryption.
- “Trusted Execution Environment.” *Wikipedia*, Wikimedia Foundation, 1 Nov. 2021, https://en.wikipedia.org/wiki/Trusted_execution_environment.
- “Levenshtein distance.” *Wikipedia*, Wikimedia Foundation, 1 Nov. 2021, https://en.wikipedia.org/wiki/Levenshtein_distance
- “ISO-8601”, *Wikipedia*, Wikimedia Foundation, 21 Dec. 2021, https://en.wikipedia.org/wiki/ISO_8601
- “tbDEX protocol for discovering liquidity and exchanging assets”, 09 Jan. 2022, https://tbdex.io/whitepaper.pdf
- “USTRWG Travel Rule Solution White Paper Version 1.0”, 24 Feb. 2022, https://web.archive.org/web/20210203091033/https://www.gdf.io/wp-content/uploads/2020/10/USTRWG-Travel-Rule-Solution-V1.pdf
- “E.164”, *Wikipedia*, Wikimedia Foundation, 21 Dec. 2021, https://en.wikipedia.org/wiki/E.164

Appendix

GlobaliD

GlobaliD is a trust platform enabled by ***decentralized identity***. Consumers create their self-sovereign digital identities and add verified credentials to them. When requested, they can share their digital credentials with 3rd parties through a Vault which secures shared information. 3rd parties can download the information directly from the Vault because a key was shared with them by the consumer.

GlobaliD also provides the service of ***managed*** identities. These are identities which are created by 3rd party custodians of consumer information such that the custodian and not the consumer controls the identity. For example, the user can sign up for a service without a self-sovereign GlobaliD identity. They can follow the custom sign up process and provide their information to the service directly. The service, being a customer of GlobaliD, may choose not to store consumer's information themselves but create a managed identity for this consumer in GlobaliD. Eventually the consumer can **claim** this managed identity to take custodial ownership of their own KYC credentials. Either way, the service will maintain access to consumer's information by storing a key to the protected KYC credential in the Vault.

AnChain.AI

AnChain.AI is an AI-powered cybersecurity company enhancing blockchain security, risk, and compliance strategies. AnChain.AI, San Jose, California, was founded in 2018 by cybersecurity and enterprise software veterans from FireEye and Mandiant. Backed by both Silicon Valley and Wall Street VCs, and selected in the Berkeley Blockchain Xcelerator, the company is trusted by 100+ customers from over 10+ countries in these sectors: VASPs, financial institutions and government, including the SEC (Securities and Exchange Commission). Featured by CBS News, MIT Tech Review, Coindesk and DEFCON, AnChain.AI's AML engine screens over $1 billion in daily crypto transactions