Crypto Valley

www.cryptovalley.swiss

CVA RESEARCH JOURNAL

2023

DON'T TRUST, VERIFY.
RISK MANAGEMENT IN WEB3

7.4. How the Travel Rule Protocol (TRP) Addresses the Challenges Presented by the Travel Rule

AUTHORS:

Nicole Giani

21 ANALYTICS

Dominik Spicher

21 ANALYTICS

HOW THE TRAVEL RULE PROTOCOL (TRP) ADDRESSES THE CHALLENGES PRESENTED BY THE TRAVEL RULE

Nicole Giani
Dominik Spicher

ABSTRACT

Nicole Giani & Dominik Spicher: How The Travel Rule Protocol (TRP) Addresses The Challenges Presented By The Travel Rule

With the growing adoption of the Financial Action Task Force's (FATF) Travel Rule and the EU's Transfer of Funds Regulation (TFR), virtual asset service providers (VASPs) have been presented with a handful of challenges.

This paper will illustrate how the Travel Rule Protocol (TRP) addresses the challenges posed by Travel Rule compliance and ensures seamless integration within existing technological solutions.

Firstly, it elucidates how TRP deployment results in seamless compliance with the FATF's Travel Rule and the EU's Transfer of Funds Regulation that respects data protection and risk mitigation requirements common to the financial services industry.

After that, it describes how the TRP framework, supported by a case study, displays the protocol's decentralised and open-source nature and allows for easy implementation for developers due to its free development tools and the fact that it is built using existing and familiar technologies.

Thirdly, the paper will focus on TRP's ability to circumvent sensitive data issues and facilitate peer-to-peer communication, ensuring that privacy and security remain paramount. It introduces the Travel Address, which effectively solves the VASP discovery problem, bolstering the efficiency of the compliance process.

In conclusion, this paper will demonstrate how TRP emerges as a transformative solution aligning with the tenets of the FATF Travel Rule and TFR requirements via its steadfast commitment to decentralisation, open-source principles, permissionless access, and user-centricity.

TRP bridges the gaps between compliance and innovation and propels the financial ecosystem towards a future of integrity, security, and interconnectivity.

Through its multifaceted approach, TRP pioneers a new era of compliance, where data verification, risk management, and global cooperation coalesce to reshape the contours of modern finance.

TABLE OF CONTENTS PAGE

1. LIST OF FIGURES

2. LIST OF ABBREVIATIONS

AML	Anti-money Laundering
CASP	Crypto Asset Service Provider
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
IVMS	InterVASP Messaging Standard
KYC	Know Your Customer
KYV	Know Your VASP
SAR	Suspicious Activity Reporting
TA	Travel Address
TFR	Transfer of Funds Regulation
TRP	Travel Rule Protocol
VASP	Virtual Asset Service Provider

3. CHAPTER 1: TRP DOESN'T TRUST; IT VERIFIES TO MEET TRAVEL RULE COMPLIANCE STANDARDS

3.1 Compliance Standards Explained

Anti-money laundering (AML) standards and recommendations like the Financial Action Task Force's (FATF's) Travel Rule are designed to prevent and detect illegal activities, such as money laundering and terrorist financing, within the financial sector. The *don't trust, verify* principle is also highly relevant in AML and Travel Rule compliance.

Below, we elucidate how the *don't trust, verify* principle is emphasised by AML and Travel Rule standards, followed by their ties to the Travel Rule in section 3.2. *Travel Rule Requirements.*

3.1.1. Customer Due Diligence

The Travel Rule requires virtual asset service providers (VASPs) to conduct thorough customer due diligence (CDD), which includes verifying the identity of customers through government-issued identification documents, verifying the source of funds, and assessing the risk associated with each customer.

3.1.2. Enhanced Due Diligence

For high-risk customers, these standards often mandate enhanced due diligence (EDD), which includes more rigorous verification processes and ongoing monitoring—ensuring that VASPs do not blindly trust but verify the legitimacy of high-risk clients.

3.1.3. Transaction Monitoring

VASPs are required to implement systems for real-time or post-transaction monitoring, as per the FATF and Transfer of Funds Regulation's (TFR's) Travel Rule. Suspicious transactions are flagged for further investigation. The focus is verifying the legitimacy of transactions to prevent illicit money flows.

3.1.4. Suspicious Activity Reporting

If VASPs identify suspicious transactions or activities, they are legally obligated to file suspicious activity reports (SARs) with the appropriate regulatory authorities. This reporting requirement manifests the "*verify*" aspect of these standards to alert authorities to potential wrongdoing.

3.1.5. Record-keeping

VASPs are mandated to maintain accurate and comprehensive customer information and transaction records. This practice ensures that there is a trail of verified information to follow in case of an investigation.

3.1.6. Ongoing Monitoring

VASPs are required to continuously monitor their customers and their activities. This ongoing vigilance ensures that institutions don't trust their own initial assessment but continually verify their customers' legitimacy and transactions.

3.1.7. Beneficial Ownership Disclosure

With AML standards and the implementation of the Travel Rule, VASPs are required to identify and verify the beneficial owners of legal entities, such as corporations and trusts, when onboarding them. This promotes transparency and helps prevent the misuse of legal entities for money laundering.

3.1.8. Technology and Automation

Many VASPs use advanced technologies, including artificial intelligence and machine learning, to improve AML compliance. These technologies help verify claims based on vast amounts of data quickly and accurately, reducing reliance on manual processes.

In summary, AML standards and the Travel Rule emphasise the *don't trust, verify* principle by requiring VASPs to implement rigorous CDD, transaction monitoring, and reporting processes. They promote the verification of customer identities, the legitimacy of transactions, and the ongoing vigilance necessary to prevent and detect money laundering and illicit financial activities.

3.2. Travel Rule Requirements

The FATF Travel Rule, as explained by the FATF (2018), serves the primary purpose of assisting law enforcement authorities in monitoring individuals engaged in fund transmissions through authorised payment systems, thereby acting as a deterrent against illicit financial activities and facilitating the identification, investigation, and prosecution of money laundering, violations of sanctions, and other forms of illicit financial conduct.

3.2.1. The FATF's Travel Rule Requirements

Initially only applicable to fiat wire transfers, the Travel Rule underwent an expansion in response to the advancements in digital technology and the growing popularity of cryptocurrencies.

In 2018, the FATF introduced amendments to its Recommendations, explicitly addressing financial activities involving virtual assets and VASPs while providing comprehensive definitions for these terms. It is noteworthy that the FATF Travel Rule, while constituting a recommendation, holds legal force upon implementation by individual jurisdictions, and numerous jurisdictions have indeed adopted and followed the FATF's suggestions regarding the Travel Rule.

The FATF (2019) put forward Recommendation 16, extending the purview of the Travel Rule to encompass virtual assets. This recommendation specifically mandated the enforcement of the Travel Rule in several scenarios, including

- conventional wire transfers,
- transfers involving virtual assets between VASPs and other obligated entities, as well as
- transfers between VASPs and self-hosted wallets.

It is important to note that while the FATF put forth these specifications above, jurisdictions are free to interpret and implement them as seen fit. For instance, the TFR instructs CASPs to obtain Travel Rule data on the transfer’s originator and beneficiary in the event of a self-hosted wallet transfer, whereas the USA’s implementation does not; in fact, it does not include self-hosted wallets within its scope.

Furthermore, it is up to the implementing jurisdiction to decide if the Travel Rule data is to be merely collected or collected and exchanged.

VASPs are defined by the FATF (2021:109) as organisations or individuals operating on behalf of others, engaging in various activities related to virtual assets, such as exchanges between virtual assets and fiat currencies, interchanges among multiple virtual assets, the transfer of virtual assets, safekeeping and administration of virtual assets, and participation in financial services linked to the issuance and sale of virtual assets.

Within this context, VASPs must ascertain the control of **the destination address for funds** (where the funds are being sent or received from), ensuring avoidance of sanctioned entities or individuals. The fundamental principle of *don't trust, verify* guides these operations, with requisite **data exchange occurring before transaction execution**.

Verification criteria encompass the originator's:

- name,
- account number,
- physical address, national identity number, customer identification, or date and place of birth, as verified by the Originator VASP.

Similarly, the beneficiary VASP is tasked with verifying the beneficiary's name and account number to ensure compliance with the Travel Rule's stipulations. (FATF:2021, p.57).

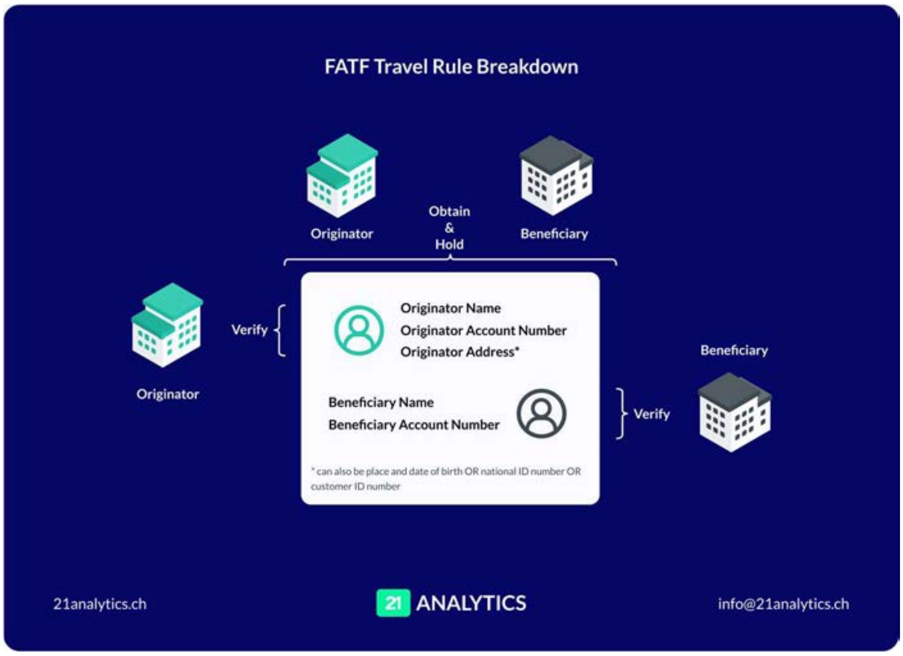


Figure 1: FATF Travel Rule Breakdown. Source 21 Analytics

3.2.2. The TFR's Travel Rule Requirements

In July 2021, the European Commission introduced an AML action plan that established a pan-European AML supervisory body. This initiative sought to standardise AML regulations across the European Union's 27 Member States and expand the scope of anti-financial crime obligations to encompass all CASPs (VASPs).

Subsequently, on 29 June 2022, a provisional agreement was reached between the European Parliament, Council, and Commission concerning the revised TFR. The primary objective of this Regulation is to implement the Recommendations of the FATF, specifically Recommendation 16.

As mentioned above, the Travel Rule applied exclusively to traditional wire transfers; however, with this regulatory development, it is extended to encompass virtual asset transfers involving crypto asset service providers (CASPs) operating within the European Union. Importantly, this Regulation is set to directly apply to all CASPs within EU member countries, eliminating the need for transposition into local legislation. (21 Analytics:2022).

To summarise, a business qualifies as a CASP if it offers any of the following services to European Union citizens:

- providing custody and management services for crypto assets on behalf of a third party,
- offering cryptocurrency exchange services or operating a cryptocurrency exchange,
- providing cryptocurrency advisory services or offering information categorised as advice related to investing in cryptocurrency assets (this definition excludes portfolio management services). ("Is a VASP a CASP?," 2022).

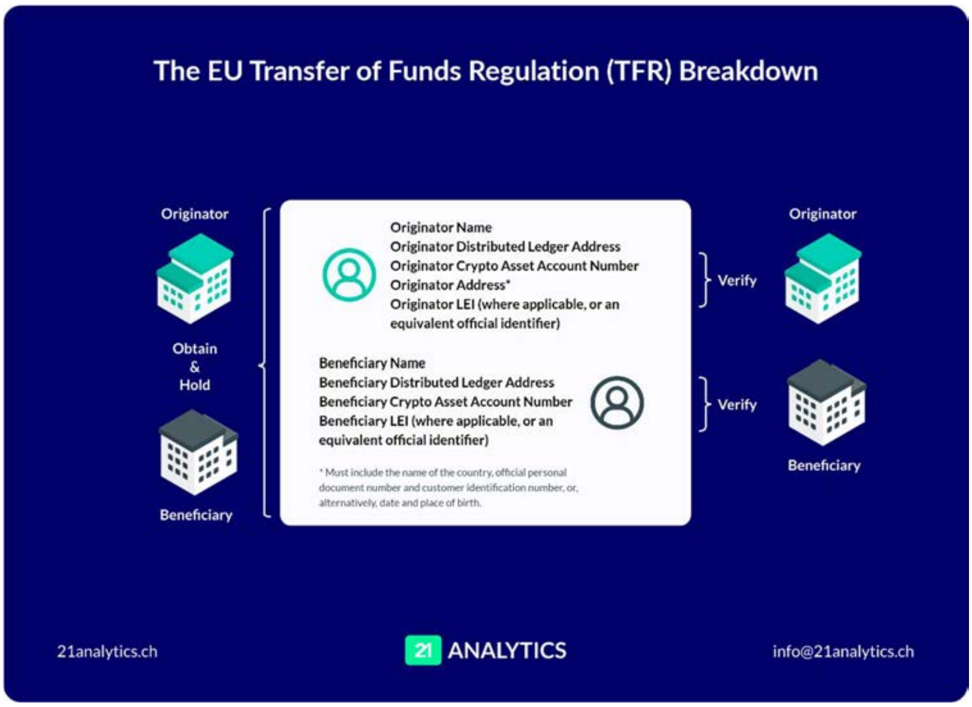
In essence, the core elements remain consistent within the context of the FATF's Travel Rule framework. Firstly, a prescribed list of data must be exchanged, encompassing various key details. The European Parliament (2023. p.16) lists these details as:

Originator data, which includes

- name,
- distributed ledger address,
- crypto asset account number,
- address, which must include the name of the country, official personal document number and customer identification number, or date and place of birth,
- LEI (where applicable, or an equivalent official identifier).

Beneficiary data, which includes

- name,
- distributed ledger address,
- crypto asset account number,
- LEI (where applicable, or an equivalent official identifier).



The EU Transfer of Funds Regulation (TFR) Breakdown

Originator Name
Originator Distributed Ledger Address
Originator Crypto Asset Account Number
Originator Address*
Originator LEI (where applicable, or an equivalent official identifier)

Beneficiary Name
Beneficiary Distributed Ledger Address
Beneficiary Crypto Asset Account Number
Beneficiary LEI (where applicable, or an equivalent official identifier)

* Must include the name of the country, official personal document number and customer identification number, or, alternatively, date and place of birth.

Figure 2: The EU Transfer of Funds (TFR) Breakdown. [Source 21 Analytics](#)

Additionally, a robust understanding of the counterparty, often requiring EDD, is imperative to ensure compliance. Equally critical is the **timing of data transmission**, as the **release of funds is contingent upon the receipt and verification of this essential information**. It is noteworthy that the intricacies of the General Data Protection Regulation must be observed during this process. Furthermore, self-hosted wallets are included in the TFR framework.

Like the FATF's Travel Rule requirement, which it is supposed to implement, the TFR stipulates the need for data to be verified and received before the transfer of virtual assets can occur—reiterating the notion of *verification over trust*: a pivotal element in the Travel Rule. (The European Parliament:2023. p.17).

As seen above, the need for VASPs to implement rigorous CDD, transaction monitoring, and reporting processes is paramount to comply with AML policies and the Travel Rule.

At any but the smallest scales, this involves the use of technological solutions. This introduces a new burden on VASPs: They need to ensure that their technological tools are actually compliant with relevant policies. As we will see, this is often not the cases. (These deficiencies will be explained in section 3.3, followed by a discussion of how TRP counters these deficiencies in section 3.4.)

This again highlights the theme of *don't trust, verify* - if technological solutions are not compliant, VASPs cannot engage in compliant business practices.

3.3. Deficiencies in Travel Rule Solutions

Based on the above commentary, many of the available Travel Rule solutions lack the required fundamentals to ensure Travel Rule compliance, resulting in a failed attempt at risk management, often succinctly summarised as *trusting without verification*. Examples of these failures will be elaborated upon below.

3.3.1 Travel Rule Information Not Exchanged as per Regulations

The originating VASP must validate and furnish the subsequent details, as seen in Figure 1, page 9, before initiating a transaction:

- originator's full name,
- originator's account number,
- either the originator's physical address or their national identity number, customer identification, or their date and place of birth.

Furthermore, the beneficiary VASP must obtain and verify the following information prior to conducting any transactions:

- beneficiary's complete name,
- beneficiary's account number.

The verification process is a crucial facet within the integral components of the Travel Rule. In order to execute the Travel Rule efficiently, this information should be communicated to the beneficiary VASP and securely retained. Care needs to be taken to ensure this data is not exposed.

If this data is not exchanged, VASPs cannot release the assets.

3.3.2 Incorrect Timing of Data

A further concern emerging in Travel Rule software pertains to the temporal aspect of Travel Rule information exchange. The Travel Rule's principal aim is to empower VASPs to promptly respond to potentially dubious virtual asset transfers, thus imposing stringent timing requirements for data transmission. Consequently, Travel Rule data should be disseminated prior to or concurrently with the transaction execution in strict adherence to regional data protection regulations to ensure secure handling.

3.3.3 Allowing Transfers to Sanctioned Addresses and Countries

The FATF Travel Rule (2021:p.62) and implementations thereof mandate originators and beneficiaries to know where the funds are being sent to or received to avoid receiving funds from sanctioned addresses and sanctioned counties.

Therefore, Travel Rule solutions need a means for users to verify this information before sensitive Travel Rule data exchanges and the release of assets.

Many solutions do not have this functionality, resulting in virtual asset transfers on behalf of sanctioned entities.

3.3.4. Absent VASP Discovery

As explained above (section 3.3.3), individuals and entities cannot send and receive funds to and from unknown VASPs, reiterating *don't trust, verify*.

In regular instances, as seen in a bitcoin address, no information is provided besides the currency. In other words, no additional information - which is pertinent to make a Travel Rule compliant and low-risk transfer - is provided.

3.3.5. Insufficient Due Diligence

With the exchange of an address alone, VASPs cannot conduct sufficient due diligence.

- They cannot ascertain if the funds are being sent to a self-hosted wallet or VASP, as explained in 3.3.4.
- They cannot check if the beneficiary has been KYVed before sharing further information or if it has been sanctioned.

The recent FATF Virtual Assets Contact Group (VACG) displayed its concern at the increased number of shell VASPs (parasite VASPs) used to conduct illicit activities.

> *"The use of shell VASPs to conduct illicit activities has been discussed as a problem, and it is essential for VASPs to detect whether a shell VASP is using their services. In short, a shell VASP (also known as parasite VASP) uses a regulated VASP's services to offer VASP services to sanctioned parties".* ("FATF Virtual Assets Contact Group (VACG): 21's Takeaways", 2023).

3.3.6. Insufficient Virtual Asset Support

The Travel Rule is all-encompassing, extending its applicability to **every virtual asset**. Consequently, any Travel Rule-compliant solution must encompass all virtual assets and provide the requisite Travel Rule data alongside each transaction. If a virtual asset is not supported by the solution, the software must decline such transactions as it is not Travel Rule compliant. It is essential to underscore that transactions must not proceed without including Travel Rule data.

3.4. TRP Doesn't Trust; It Verifies to Meet Travel Rule Compliance Standards

The FATF Travel Rule is the epitome of *don't trust, verify* with its requirement of data collection, verification and storage to ensure safe transactions, and as such, it requires a protocol that can meet this need.

As seen repeatedly with failed exchanges, one cannot trust the information gleaned from one's counterparty. The information must be verified via trustworthy and reliable means, such as protocols like TRP.

TRP effectively addresses the aforementioned shortcomings within the virtual asset transaction space. When initiating a transaction through TRP, VASPs are prompted to input customer Travel Rule information strictly per the Travel Rule requirements before proceeding.

Furthermore, TRP offers VASPs the capability to authorise or reject inbound transactions (21 Analytics:2022) prior to any on-chain activities, ensuring comprehensive Travel Rule compliance. This is enforced on a protocol level by sharing blockchain destination addresses only once the supplied Travel Rule data has been deemed satisfactory. This feature is especially advantageous for VASPs not engaging in transactions involving specific currencies, as it facilitates swift rejection procedures.

Additionally, all transactions facilitated by TRP include internal account numbers and postal addresses, positioning the protocol as the most Travel Rule-compliant software available in the current landscape.

It is important to emphasise that TRP is one of the sole protocols in full adherence to FATF Recommendations due to its functionalities, further discussed in section 4.3, the TRP Flow. Its attributes encompass a global perspective, allowing VASPs to operate without being tied to any jurisdiction.

In section 4, TRP's framework and design will be discussed to illustrate its seamless integration into existing solutions and technologies, ensuring familiarity and ease of implementation for IT and development teams.

TRP is permissionless, decentralised, and open-source, enabling unrestricted contribution to its development and implementation, free from dependencies on specific entities or gatekeepers.

In tangent, the FATF remarked that the Travel Rule has not been widely adopted by low-resource countries; one of the rationals is the cost of Travel Rule software and protocols.

Therefore, the FATF has recognised the significance of enabling low-resource countries to engage in the virtual asset arena and has designated them as a primary focus.

To facilitate their participation, the FATF is encouraging the development and adoption of open-source protocols and solutions, like TRP. (Cited in 21 Analytics:2023).

4. CHAPTER 2: TRP: AN OPEN-SOURCE STANDARD

4.1. TRP Adherers to the *Don't Trust, Verify* Principle

Several key concepts and techniques can be applied to make a protocol or system adhere to the concept of *don't trust, verify*. TRP was designed under these principles.

4.1.1. Open Source and Transparent

The protocol's specification is open for inspection and auditing. Transparency allows anyone to review the code, find vulnerabilities, and ensure no hidden backdoors or malicious components.

4.1.2. Decentralisation and Permissionless Access

Decentralisation was achieved through the distribution of control and verification responsibilities among multiple parties or nodes. Within the protocol, no privileged party exists between the originator and beneficiary VASPs and may act as a gatekeeper. This is in stark contrast to numerous other Travel Rule protocols that have been proposed.

4.1.3. Auditing and Third-Party Verification

Independent security auditors and experts have reviewed and verified the security and integrity of the protocol, adding an additional layer of trustworthiness.

4.1.4. Permissionless and Trustless Systems

The protocol was designed to be permissionless and trustless. In a trustless system, participants can interact without having to trust a central authority.

4.1.5. Community Involvement

TRP calls for active community participation in the development and verification of the protocol.

By implementing these principles and techniques, a protocol can work towards meeting the *don't trust, verify* standard, enhancing security, transparency, and trustworthiness in various domains, including blockchain, cybersecurity, and beyond.

4.2. Tools and Libraries to Accompany TRP

TRP was designed with various open-source tools and libraries readily available for development teams tasked with implementing the Travel Rule Protocol. These resources afford developers comprehensive access to the underlying source code, promoting transparency and ease of integration into TRP-related projects.

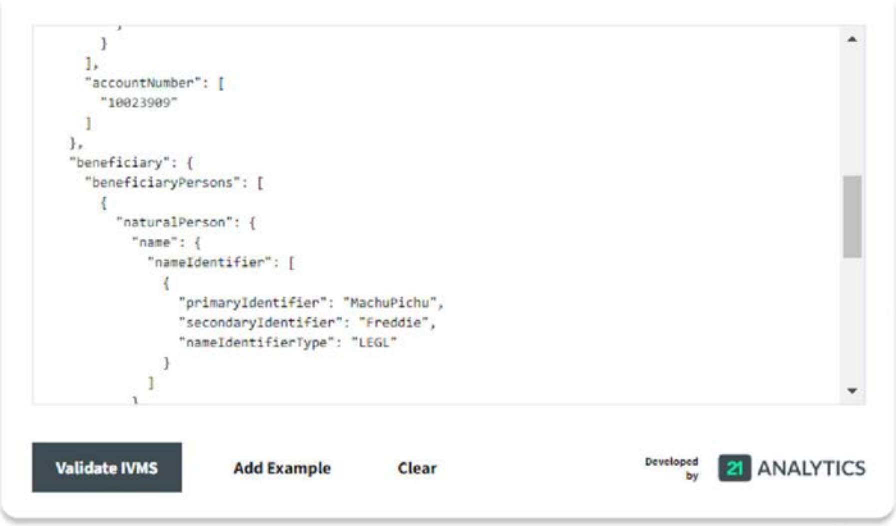
Sections 4.2.1 - 4.2.3 are intended to offer a brief overview of these tools, which will be revisited in later chapters. The purpose is to give the reader a basic understanding of these tools.

4.2.1. The IVMS Validator and Open-source Library

Developers can use the IVMS 101 Validator to assess the compatibility of input data with the IVMS 101 data model standard, a framework used within the context of the TRP.

The open-source IVMS library aids faster and broader adoption of TRP through straightforward integration into existing software.

- Example of protocol flow: https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/master/core/specification.md#detailed-protocol-flow
- IVMS Library source code: gitlab.com/21analytics/ivms101



```
      }
    ],
    "accountNumber": [
      "10023909"
    ]
  },
  "beneficiary": {
    "beneficiaryPersons": [
      {
        "naturalPerson": {
          "name": {
            "nameIdentifier": [
              {
                "primaryIdentifier": "MachuPichu",
                "secondaryIdentifier": "Freddie",
                "nameIdentifierType": "LEGL"
              }
            ]
```

Figure 3: IVMS Validator with Example. Source 21 Analytics

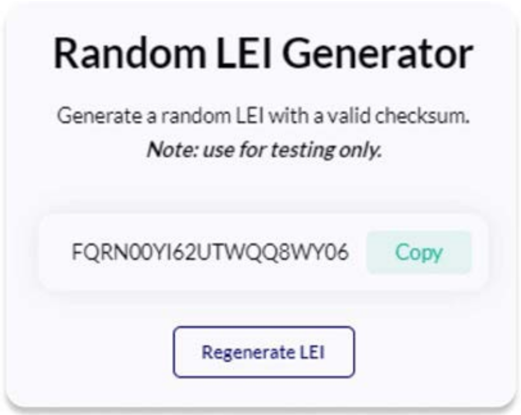
4.2.2. The LEI Generator and Open-source Library

TRP uses the "nationalIdentification" field of IVMS 101 for identifying the originating VASP, and for the "nationalIdentifierType", LEIs are used.

The LEI Generator allows developers to create dummy LEI codes which can be used to test products and software.

The open-source LEI library permits developers to use and modify the code according to their needs. Additionally, LEIs are required to be exchanged per the TFR. Therefore, they form a part of TRP's foundation.

- LEI Library source code: gitlab.com/21analytics/lei
- LEI specification: https://www.gleif.org/en/about-lei/iso-17442-the-lei-code-structure
- LEI search: https://search.gleif.org



Random LEI Generator

Generate a random LEI with a valid checksum.

Note: use for testing only.

FQRN00YI62UTWQQ8WY06

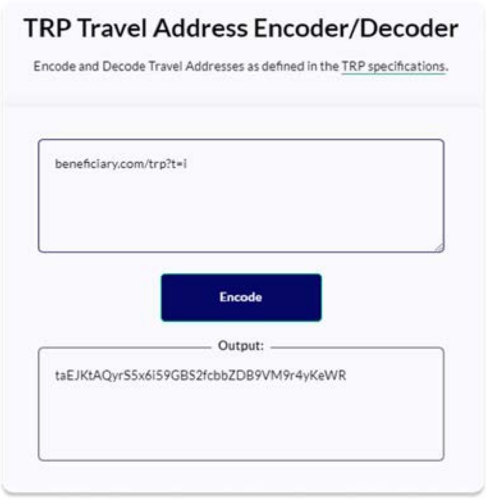
Figure 4: Random LEI Generator. Source 21 Analytics

4.2.3. The TRP Travel Address Encoder/Decoder

This tool lets users see exactly what information a Travel Address comprises.

A Travel Addresses allows VASPs to identify their counterparty VASP as it confirms which VASP controls the receiving address and the VASP's URL to receive Travel Rule data, data not present in a "normal" address.

A Travel Address is a URL encoded in the base58 format, housing a unique URL. Once the originating VASP deciphers the Travel Address, it initiates a request to the associated URL to seek authorisation for transaction execution.



TRP Travel Address Encoder/Decoder

Encode and Decode Travel Addresses as defined in the TRP specifications.

beneficiary.com/trp?t=i

Encode

Output:

taEJKtAQyrS5x6i59GBS2fcbbZDB9VM9r4yKeWR

Figure 5: TRP Travel Address Encoder/Decoder with Example. Source 21 Analytics

4.3. The TRP Flow

A VASP using TRP will conduct a Travel Rule-compliant transaction due to the careful verification processes of TRP.

As demonstrated above, TRP uses existing technologies, such as IVMS101 and LEIs, to ascertain customer data and the Travel Address to identify the beneficiary VASP, resulting in additional verification processes, which many other protocols do not factor into the data verification process.

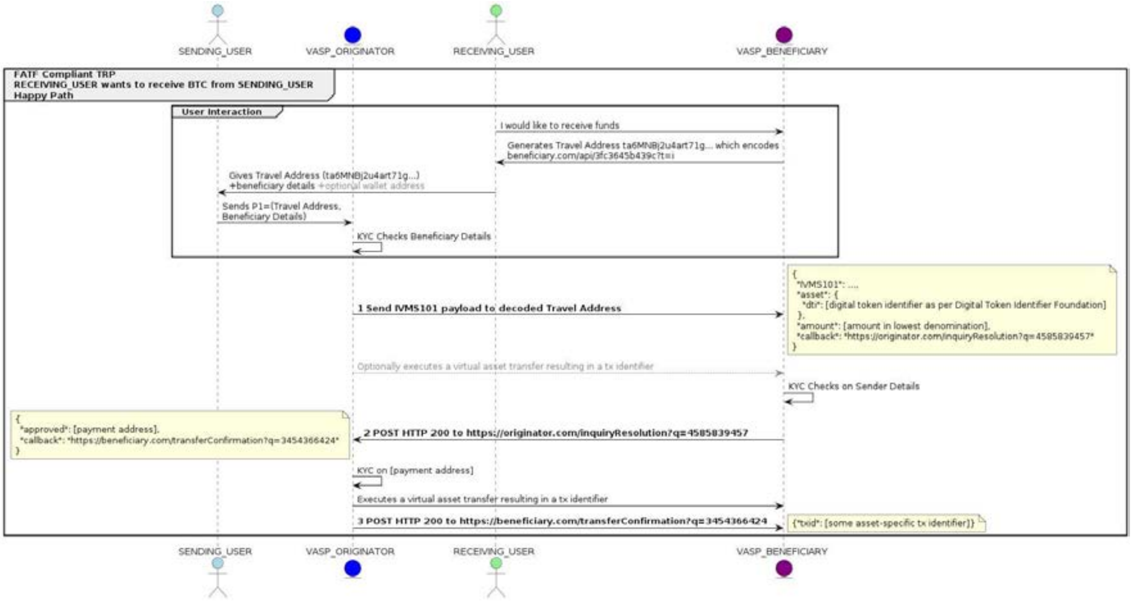

SENDING_USER
VASP_ORIGINATOR
RECEIVING_USER
VASP_BENEFICIARY
FATF Compliant TRP
RECEIVING_USER wants to receive BTC from SENDING_USER
Happy Path
User Interaction
I would like to receive funds
Generates Travel Address ta6MNBj2u4art71g... which encodes beneficiary.com/api/3fc3645b439c?t=i
Gives Travel Address (ta6MNBj2u4art71g...) +beneficiary details +optional wallet address
Sends P1=(Travel Address, Beneficiary Details)
KYC Checks Beneficiary Details
1 Send IVMS101 payload to decoded Travel Address
{ "IVMS101": ...., "asset": { "dti": [digital token identifier as per Digital Token Identifier Foundation] }, "amount": [amount in lowest denomination], "callback": "https://originator.com/inquiryResolution?q=4585839457" }
Optionally executes a virtual asset transfer resulting in a tx identifier
KYC Checks on Sender Details
2 POST HTTP 200 to https://originator.com/inquiryResolution?q=4585839457
{ "approved": [payment address], "callback": "https://beneficiary.com/transferConfirmation?q=3454366424" }
KYC on [payment address]
Executes a virtual asset transfer resulting in a tx identifier
3 POST HTTP 200 to https://beneficiary.com/transferConfirmation?q=3454366424
{"txid": [some asset-specific tx identifier]}
SENDING_USER
VASP_ORIGINATOR
RECEIVING_USER
VASP_BENEFICIARY

Figure 6: TRP Flow. Source Travel Rule Protocol GitLab Repository

Participants:

Sender: Ori
Receiver: Ben
Originating VASP: VASP O
Beneficiary VASP: VASP B

Objective:

Ben intends to receive bitcoin (BTC) from Ori, and both parties use VASPs to facilitate this transaction.

Actions Taken by Ben and Ori:

- Ben, the beneficiary, communicates his desire to receive BTC from Ori to his VASP.
- The beneficiary's VASP (VASP B) initiates the process by generating a TA and giving it to Ben.
- Ben, as the beneficiary, sends the generated TA to Ori.
- In his role as the originator, Ori conveys this TA to his VASP (VASP O) along with beneficiary details (like Ben's name).

Behind the Scenes Processing:

- Ori's VASP undertakes a sanctions and politically exposed person (PEP) check to verify the details of the beneficiary (Ben).
- If the beneficiary's details are found to be in order, an IVMS payload is sent to the decoded Travel Address. VASPs could use the Travel Address Encoder/Decoder described in section 4.2.3.
- Subsequently, VASP B carries out a sanctions and PEP check on Ori, the sender.
- If Ori's details are deemed satisfactory, VASP B transmits a crypto address to VASP O.
- Ori's VASP (VASP O) optionally runs the provided address through an on-chain analytics tool and executes the transfer.
- The Transaction ID is then sent to VASP B, concluding the transfer.

4.4. A TRP Case Study: The Implementation of TRP and the Challenges Faced

TRP is less complex to implement than most Travel Rule protocols as it uses existing technology building blocks that IT and development teams are familiar with. Below, a case study is presented, which explores the experience of Blockchain Intelligence Group's* (BIG) implementation of the TRP and the challenges encountered during the process. The TRP is a critical protocol for the cryptocurrency industry, designed to address regulatory requirements for transferring customer information between VASPs during cryptocurrency transactions.

Implementation of TRP

BIG embarked on the implementation of TRP to comply with emerging regulatory requirements in the cryptocurrency sector. The institution was keen on evaluating whether TRP effectively addressed the challenges presented by the Travel Rule.

Addressing Travel Rule Challenges

The institution's perspective on TRP was positive. When asked if TRP addressed the Travel Rule's challenges, the response was affirmative. The implementation of TRP was seen as a step in the right direction towards ensuring compliance with Travel Rule requirements.

Implementation Ease and Challenges

The implementation process was generally regarded as straightforward. However, the institution encountered several challenges during the implementation, which were seen as potential roadblocks:

a) Handling KYC Rejections

A challenge was the absence of direct calls for acknowledging the counterparty VASP in the event of Know Your Customer (KYC) rejections. The institution was uncertain if this was the common practice within the banking system. However, the absence of a clear mechanism for handling KYC rejections meant that the counterparty VASP was left waiting for a response, potentially causing delays and uncertainties in the transaction process.

b) Use of Development Tools and Libraries

The institution leveraged development tools and libraries from 21 Analytics, including the IVMS validator and LEI library. However, a notable hurdle was the use of a different programming framework other than Rust. Nevertheless, the institution expressed an interest in the availability of these tools in various languages, particularly in Java, given its widespread use in fintech applications and banking systems.

Conclusion

In conclusion, BIG's implementation of TRP was generally seen as a positive step towards addressing Travel Rule challenges. The institution recommended the development of TRP tools and libraries in multiple programming languages to facilitate broader industry adoption. Despite the challenges, the institution expressed gratitude for the assistance received during the implementation and emphasised its commitment to compliance with evolving cryptocurrency regulations.

> **"Blockchain Intelligence Group builds technology to power compliance and intelligence for the blockchain-centric future. Leaders use our solutions to transact cryptocurrency or power complex investigations into criminal activity using digital currencies. Banks and crypto companies depend on our technology to monitor risk from crypto transactions. Investigators and law enforcement quickly identify and track illicit activity."* ("Blockchain Intelligence Group: About Us", 2021)

5. CONCLUSION

In conclusion, TRP exemplifies a compelling model for adequate adherence to AML standards and the Travel Rule, underpinned by a rigorous implementation of the *don't trust, verify* principle. This protocol harmoniously integrates meticulous procedural protocols and state-of-the-art technological advancements to ensure the highest echelon of compliance, emphasising the perpetual verification of transactional legitimacy and customer engagement.

TRP demonstrates an unwavering commitment to the core tenets of CDD, characterised by its insistence upon exacting identity validation procedures, and the persistent scrutiny and validation of customer information and transactional conformity to EDD protocols are judiciously applied in cases of heightened risk, amplifying the verification process when requisite.

In real-time, the salient transaction monitoring and prompt reporting of suspicious activities encapsulate the fundamental "verify" paradigm inherent to AML regulations and the Travel Rule. Transactions flagged as suspicious undergo expedient investigation and, when substantiated, are duly reported to the relevant regulatory authorities, effectively safeguarding against the potential obfuscation of money laundering endeavours.

Moreover, TRP harnesses cutting-edge technology and automated systems, facilitating the expeditious and precision-driven management and processing of substantial data volumes, thereby mitigating the inherent risks of human fallibility and streamlining the verification procedures. This embrace of technology demonstrates TRP's unwavering dedication to staying at the forefront of the ongoing fight against financial crimes.
The incorporation of beneficial ownership disclosure practices within the TRP framework fosters an environment that is notably less conducive to the surreptitious concealment of illicit activities behind corporate facades. This commitment to transparency harmonises with the overarching AML principle of validating the veritable ownership and purposes of legal entities.

In summary, TRP manifests a robust dedication to the pinnacle of AML standards, and the *don't trust, verify* maxim through meticulous CDD practises, the vigilant monitoring of transactions, the prudent integration of advanced technology, and an unwavering commitment to regulatory oversight. In adopting these measures, TRP not only enhances its own integrity but also substantively contributes to the broader mission of curtailing money laundering and illegitimate financial practices.

6. APPENDIX I: DEFINITIONS

Term	**Definition**
Beneficiary	Where virtual assets are being sent to. It can be a person or entity.
Decentralised	A system, organisation, or network structure where control, authority, or decision-making is not concentrated in a central authority or entity but is instead spread among multiple independent nodes or participants. There is no single entity with ultimate control.
Financial Action Task Force (FATF)	*"The Financial Action Task Force (FATF) leads global action to tackle money laundering, terrorist and proliferation financing. The FATF researches how money is laundered and terrorism is funded, promotes global standards to mitigate the risks, and assesses whether countries are taking effective action".* (FATF:2023)
InterVASP Messaging Standard (IVMS)	*"IVMS 101.2023 Universal common language for communication of required originator and beneficiary information between virtual asset service providers."* InterVASP Standards Working Group (2023, p1).
Legal Entity Identifier (LEI)	A unique identifier specific to a business entity. Comprised of 20 alphanumeric characters, this code facilitates the global identification of businesses within a database. When using the LEI search tool provided by the Global Legal Entity Identifier Foundation (GLEIF), the following information will be displayed: • The business's name. • Its address. • Whether the business is a subsidiary of another entity. • The location where it has been registered. (GLEIF:2023)
Open Source	Computer software distributed under a licensing arrangement where the copyright holder provides users with the freedom to use, examine, modify, and share both the software itself and its underlying source code with anyone, without restrictions on purpose.

Originator	Where virtual assets are being sent from. It can be a person or entity.
Protocol	A protocol is a collection of guidelines governing the exchange of data between various entities. It essentially functions as a specification, a formal documentation. An engineer possesses the capability to transform this specification into a tangible product.
Travel Address (TA)	The Travel Address is a string of characters used to replace a wallet address in crypto transfers. It contains the following information to allow for VASP discovery: • The VASP who controls the receiving address • The VASP's URL to receive the Travel Rule data.
Transfer of Funds Regulation (TFR)	The TFR is the European Union's implementation of the Travel Rule.
Travel Rule	The Travel Rule is an important measure in anti-money laundering and countering the financing of terrorism (AML/CFT) efforts. Its purpose is to empower VASPs and financial institutions in preventing terrorists, money launderers, and criminals from utilising wire transfers to move their funds, including virtual assets. Additionally, it aids in identifying and addressing such misuse if it occurs. The primary objective of these requirements is to ensure that originator and beneficiary information is readily accessible for the following purposes: • Assisting law enforcement authorities in detecting, investigating, and prosecuting terrorists or other criminals, as well as tracing their assets. • Facilitating financial intelligence units in analysing suspicious or unusual activities.

	• Enabling ordering, intermediary, and beneficiary VASPs and financial institutions to identify and report suspicious transactions, freeze funds, and prevent transactions involving sanctioned individuals or entities. (“What Is the FATF Travel Rule?”, 2022)
Travel Rule Protocol (TRP)	*“Short for Travel Rule Protocol, TRP is an open-source standard for exchanging crypto-asset transfer-related data between virtual asset service providers (VASPs) as required by the FATF Travel Rule Recommendation 16.*” (21 Analytics:2021)
Virtual Asset Service Provider (VASP)	As defined by the FATF (2021, p.109): *“A virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:* • *exchange between virtual assets and fiat currencies;* • *exchange between one or more forms of virtual assets;* • *transfer of virtual assets;* • *safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and* • *participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset”.*

7. APPENDIX II: HOW TO IMPLEMENT TRP

To implement TRP, developers must access the tools, libraries and links in section 4.2. Thereafter, follow the below prompts.

Step 1: Initiate a Request

1. Generate a Travel Address on Beneficiary. Note the crypto asset and beneficiary name.
2. Decode the Travel Address using the Travel Address Decoder/Encoder explained in section 4.2.3.
3. Use a sample request payload from: https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/master/core/specification.md#detailed-protocol-flow
4. Specify the callback https://workshop.21analytics.xyz/<some thing else>
5. Use the correct asset (4H95J0R2X).
6. Use the correct beneficiary name.
7. Use the correct LEI (of the VASP configured to have https://workshop.21analytics.xyz as an API endpoint, GTFZ00N6IHYMHHNT8S51).
8. Ensure that mandatory headers have been added.

Step 2: Capture the Beneficiary's Response

1. Login to https://testing.21analytics.xyz and approve the initiated transaction.
2. Go to https://workshop.21analytics.xyz/log.txt
3. Copy and paste the callback field.

Step 3: Finalise Response

1. Collect a random transaction ID. Then visit a block explorer or https://blockbook.21analytics.xyz/blocks

2. Make an HTTP POST request to the callback URL copied and pasted with the body as defined in the TRP specifications.

Lastly, to create a TRP server, cURL requests are to be used

To initiate:

- curl -v -H 'content-type: application/json' -H 'api-version: 3.2.0' -H 'request-identifier: foo' -d @ivms.json

```
'https://api.testing.21analytics.xyz/transfers/7b20efe3-e0e1-42d4-b976-1ca9d324cff1?t=i'
```

To finalise:

- curl -v -H 'content-type: application/json' -H 'api-version: 3.2.0' -H

```
'request-identifier: foo' -d '{"txid":
"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"}'
"https://api.testing.21analytics.xyz/transfers/a18f0447-3be1-450b-a48a-5a068b7850e2/conf
Irmation"
```

8. REFERENCES

European Commission. (2021). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0422

Financial Action Task Force. (2021). *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.* https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

Financial Action Task Force. (2022). *Targeted Update on Implementation of FATF's Standards on VAs and VASPs.* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Targeted-update-virtual-assets-vasps.html

Global Legal Entity Identifier Foundation. (2023). *Introducing the Legal Entity Identifier (LEI).* https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei

interVASP Standards Working Group (17 July 2023). *interVASP Messaging Standards: Working Draft.* https://www.gdf.io/wp-content/uploads/2020/12/IVMS101.2023-Working-Draft-For-Consultation.pdf

Official Journal of the European Union. (2023). *REGULATION (EU) 2023/1113 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1113

Travel Rule Protocol Specification. (2023). https://gitlab.com/OpenVASP/travel-rule-protocol/-/blob/master/core/specification.md?ref_type=heads#overview

21 Analytics. (n.d). *What Is TRP?* https://www.21analytics.ch/what-is-trp/

21 Analytics. (07.09.2021). *How the TRP Travel Address Solves the FATF Travel Rule.* https://www.21analytics.ch/blog/how-the-trp-travel-address-solves-the-fatf-travel-rule/

21 Analytics. (07.06.2022). *How TRP Allows for VASPs to Accept or Reject Transfers Before They Take Place?* https://www.21analytics.ch/blog/how-trp-allows-for-vasps-to-accept-or-reject-transfers-before-they-take-place/

21 Analytics. (26.09.2022). *Is a VASP a CASP? https://www.21analytics.ch/blog/is-a-vasp-a-casp-market-in-crypto-assets/*

21 Analytics. (04.10.2022). *What Does The Revised Transfer of Funds Regulation (TFR) Entail?* https://www.21analytics.ch/blog/what-does-the-revised-transfer-of-funds-regulation-entail/

21 Analytics. (26.04.2023). *FATF Virtual Assets Contact Group (VACG): 21's Takeaways.* https://www.21analytics.ch/blog/fatf-virtual-assets-contact-group-vacg-21s-takeaways/

21 Analytics. (01.05.2023). *The Transfer of Funds Regulation (TFR) Summarised.* https://www.21analytics.ch/blog/the-transfer-of-funds-regulation-tfr-summarised/

21 Analytics. (10.05.2023). *Deficiencies in Travel Rule Solutions.* https://www.21analytics.ch/blog/deficiencies-in-travel-rule-solutions/

21 Analytics. (25.05.2023). *TRP Workshop: Implementing the Open Travel Rule Standard.* https://www.21analytics.ch/blog/trp-workshop-implementing-the-open-travel-rule-standard/

21 Analytics. (27.06.2023). *Guidelines for Choosing Travel Rule Technological Solutions.* https://www.21analytics.ch/blog/guidelines-for-choosing-travel-rule-technological-solutions/

21 Analytics. (11.10.2023). *European Union.* https://www.21analytics.ch/travel-rule-regulations/european-union-eu-travel-rule-regulation/