Travel Rule Report

gwp incore

Introduction

The emergence of new blockchain technologies and new financial products services over the last decade has been one of the major changes to the global financial system. This new trend has brought innovation, increased efficiency and improved financial inclusion.

Cryptocurrencies and virtual assets (VA) as an accepted part of the financial markets, have attracted the attention of regulatory bodies, including the Financial Action Task Force (FATF). As an international standard setting body, the FATF sets rules for anti-money laundering, which is part of the Travel Rule that was first introduced in 2012. Those standards require the exchange of client data between financial intermediaries and are reviewed and updated in regular cycles.

This report introduces you to the Travel Rule framework, demonstrates how financial intermediaries can comply with the standards and highlights differences for countries that have implemented the rule.

Further, it gives a technical overview of existing protocols that can be implemented to comply with the Travel Rule, and highlights the main differences in order to give an idea of what to expect and what requirements need to be addressed.

November 2020

Content

1 A Global Lens on the Legal Situation

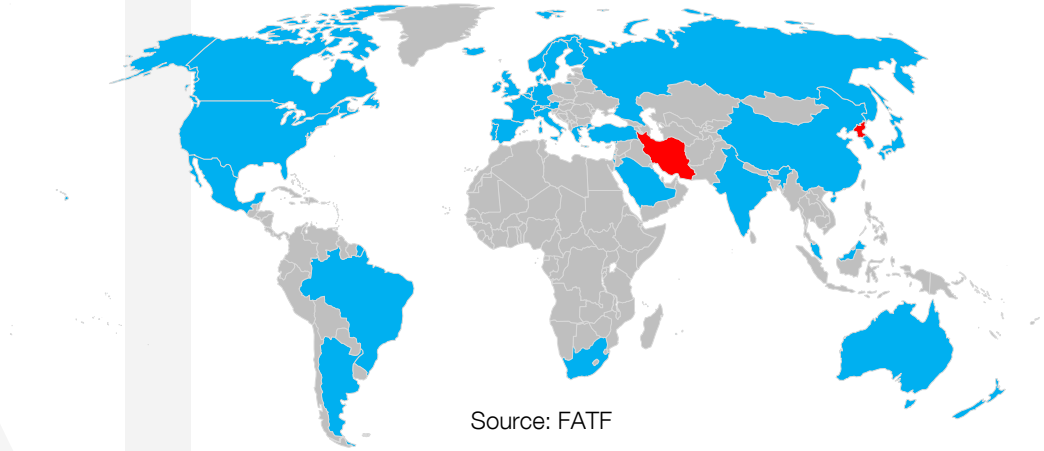
Travel Rule Evolution

The Travel Rule was first introduced in 1996 by the Financial Crime Enforcement Network (FinCEN), a U.S. federal bureau, under which banks and money services businesses must share information of both the originators and beneficiary tied to payments of $3'000 and higher. In 2012 the policy was amended to include electronic funds transfers.

FATF adopted the Travel Rule only in 2012 to its policy recommendations. By 2018 global crypto regulation gained traction and the need to apply the Travel Rule to virtual assets (VA) and virtual asset service providers (VASP) became necessary.

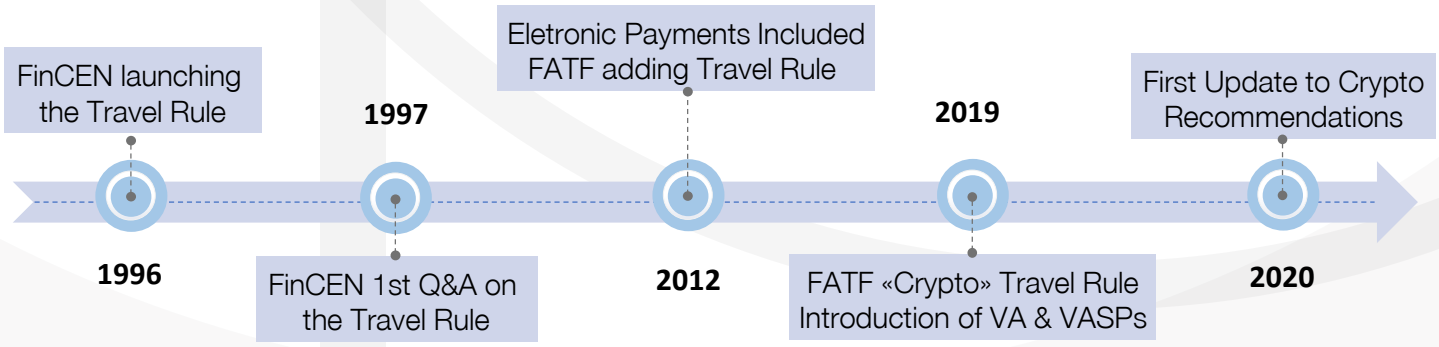
In June 2019 FATF proposed global standards regarding the sharing of beneficiary and originator information between Virtual Asset Service Providers (VASPs), inspired by regulation from FinCEN in the United States. Entities subject to these regulations are cryptocurrency exchanges, custodial wallets, DEX operators or others based on the interpretation of regulations in each jurisdiction.

FATF Member Countries (blue) & Blacklist (red)



Source: FATF

These funds transfer "rules" are designed to help law enforcement agencies to detect, investigate and prosecute money laundering and other financial crimes by preserving an information trail about persons sending and receiving funds through funds transfer systems.



Travel Rule Requirements

All of the requirements set in Recommendation 16 apply to VASPs and other obliged entities that engage in VA transfers, including the obligations to obtain, hold and transmit required originator and beneficiary information in order to identify and report suspicious transactions, monitor the availability of information, take freezing actions, and prohibit transactions with designated persons and entities.

Countries should therefore ensure that ordering institutions (VASPs or other obliged entities such as a Financial Intermediary (FI)) involved in a VA transfer, obtain and hold required and accurate originator information and required beneficiary information and submit the information to beneficiary institutions. The accurate information is set forth in the following excerpt from FATF's guidance for a risk-based approach to VA and VASPs:

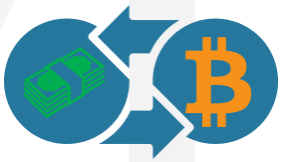
Excerpt from *FATF (June 2019),*
Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers
FATF, Paris

"The required information includes the:

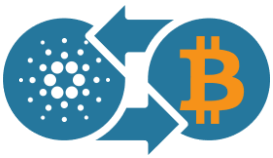
- originator's name (i.e., the sending customer);
- originator's account number where such an account is used to process the transaction (e.g., the VA wallet);
- originator's physical (geographical) address, or national identity number, or customer identification number (i.e., not a transaction number) that uniquely identifies the originator to the ordering institution, or date and place of birth;
- beneficiary's name;
- beneficiary account number where such an account is used to process the transaction (e.g., the VA wallet). It is not necessary for the information to be attached directly to the VA transfer itself. The information can be submitted either directly or indirectly, as set forth in Interpretive Note to Recommendation (INR) 15."

Defining VASPs

Service Providers qualified as a VASP:



Fiat-Crypto Exchange



Crypto Exchange

Payment Providers

Token Issuers

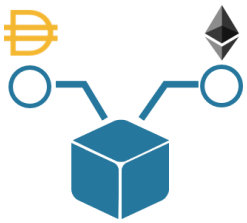
Crypto ATMs

Custodial Wallets

Crypto Funds

Service Providers that may qualify as a VASP:

P2P



DeFi

DApps

As defined by FATF, VASPs include any person or entity that provides these services as part of their business:

- Fiat and virtual asset exchange;
- Exchange between virtual assets;
- Transfer of virtual assets;
- Safekeeping of virtual assets; or
- Activities related to issuing or underwriting virtual assets.

FATF Update June 2020

In June 2019 the FATF finalised amendments to its global standards to clearly place anti-money laundering and counter-terrorism financing (AML/CFT) requirements on virtual assets and VASPs. It also agreed to undertake 12-month reviews to measure the implementation of the revised standards by jurisdictions and the private sector, as well as monitoring for any changes in the typologies, risks and the market structure of the virtual assets sector.

The FATF 12-months update report from June 2020, identified several issues with the revised FATF standards and guidance. The issues were identified through the FATF questionnaire and Virtual Assets Contact Groups.

The report notes that the new requirements are being adopted by most of the FATF member countries (including Switzerland) to combat money laundering and terrorism financing. Likewise, progress has been made in developing technological solutions for the Travel Rule. However, not all members of FATF Global network have reported a response to the amended standards by June 2020. The FATF research also found that there is still a widespread lack of Travel Rule regulatory compliance in many countries as well as cases of complete banning of the new requirements.

As jurisdictions have to transpose the revised FATF standards into their national laws, they have identified areas where there could be greater clarity in the guidance. For example in the context of so-called stablecoins, whether jurisdiction should be treating them as traditional or virtual assets. Also, there is a need for greater guidance on the scope of activities, such as safekeeping, administration of virtual assets, or transfer of assets.

More progress expected in the near-term

The next 12-month review of the crypto industry implementation of the FATF standard is set for June 2021. The FATF's next regulatory actions until June 2021 will also include case studies on red flag indicators to support the further understanding of ML/TF risks associated with the crypto industry.

Other issues that need to be reviewed include peer-to-peer transfers of virtual assets, where a VASP is not involved as an intermediary and such type of transactions are not explicitly subject to AML/CFT obligation under the revised FATF standards. The lack of explicit coverage of peer-to-peer transactions via private wallets was a source of concern for a number of jurisdictions, including Switzerland. According to the report, anonymous peer-to-peer transactions have not changed materially since June 2019. Due to the fact of insufficient evidence, the authors conclude that those peer-to-peer transactions do not pose an increased ML/ TF risk.

The launch of new virtual assets however could change the ML/TF risks, particularly if there is a mass-adoption of assets that enables anonymous peer-to peer transactions. For example, if the authorities consider the risk to be too high, they could possibly ban, deny licensing of the platforms, which allow "unhosted" wallets transfers, introduce transaction/volumes limits or mandating that the transactions with the use of a VASP.

Finding a standardised solution

In order to comply with the Travel Rule, VASPs must be able to identify when they are (a) transacting with another VASP and (b) whether the counterparty VASP is registered/licensed by a jurisdiction and adequately supervised for AML/CFT purposes. The question is how to conduct counterparty due diligence in a timely and secure manner. One way will be to create a global list of VASPs where the information will be consolidated from all jurisdictions and accessed through a coherent, central database but managed in a decentralised manner, processable by members. This proposal of the private sector raises a number of questions: who is responsible for collecting and maintaining the information (governance), who will supervise the process and who will have access.

A solution could be to delegate the responsibility of to member countries to keep a localized list of VASPs.. This option still raises the same questions, on how and by whom it should be managed. All of these requirements need to be addressed before a solution is developed.

Swiss Interpretation of the updated Travel Rule

Switzerland

FINMA Guidance 02/2019, Payments on the Blockchain: "VASPs are obliged, for example, to verify the identity of their customers, to establish the identity of the beneficial owner, to take a risk-based approach to monitoring business relationships and to file a report with the Money Laundering Reporting Office Switzerland (MROS) if there are reasonable grounds to suspect money laundering. Unlike the FATF standards, Article 10 AMLO-FINMA does not provide for any exception for payments involving unregulated wallet providers.

Such an exception would favor unsupervised service providers and would result in supervised providers not being able to prevent problematic payments from being executed."

Switzerland's high standards in regards to the compliance with the AML/CTF regulation for virtual assets implies some complicity to the Swiss intermediaries to cooperate with other jurisdictions. There are not many jurisdictions who introduce similar high standards. The exception could be Singapore (MAS, Payment Service Act, 2019) or US (FinCEN, guidance for VASPs, May 2019, which includes the application of the BSA Travel Rule). The high standard requirements and differences in approach and inconsistency of requirements in other countries impose difficulties on proper functionality and compliance of transactions between Switzerland and other counties, where the requirements for private wallets are less stricter or undefined. It will also make the transactions more expensive and not This topic requires more coverage from FATF.

VASPs are considered professional financial intermediaries, if they meet the following criteria:

a) a gross revenue of more than CHF 50,000 per calendar year;

b) established business relationships with more than 20 contractual parties who engage with the FI more than once per calendar year;

c) unlimited control of third-party funds in excess of CHF 5 million, or

d) performs transactions at a volume of more than over CHF 2 million per year.

Difference in Global Compliance Requirements

Unlike the FATF standards, Article 10 AMLO-FINMA in Switzerland does not provide for any exception for payments involving unregulated wallet providers. Such an exception would favor unsupervised service providers and would result in supervised providers not being able to prevent problematic payments from being executed.

As long as an institution supervised by FINMA is not able to send and receive the information required in payment transactions, such transactions are only permitted from and to external wallets if these belong to one of the institution's own customers. Their ownership of the external wallet must be proven using suitable technical means. Transactions between customers of the same institution are permissible. A transfer from or to an external wallet belonging to a third party is only possible if, as for a client relationship, the supervised institution has first verified the identity of the third party, established the identity of the beneficial owner and proven the third party's ownership of the external wallet using suitable technical means.

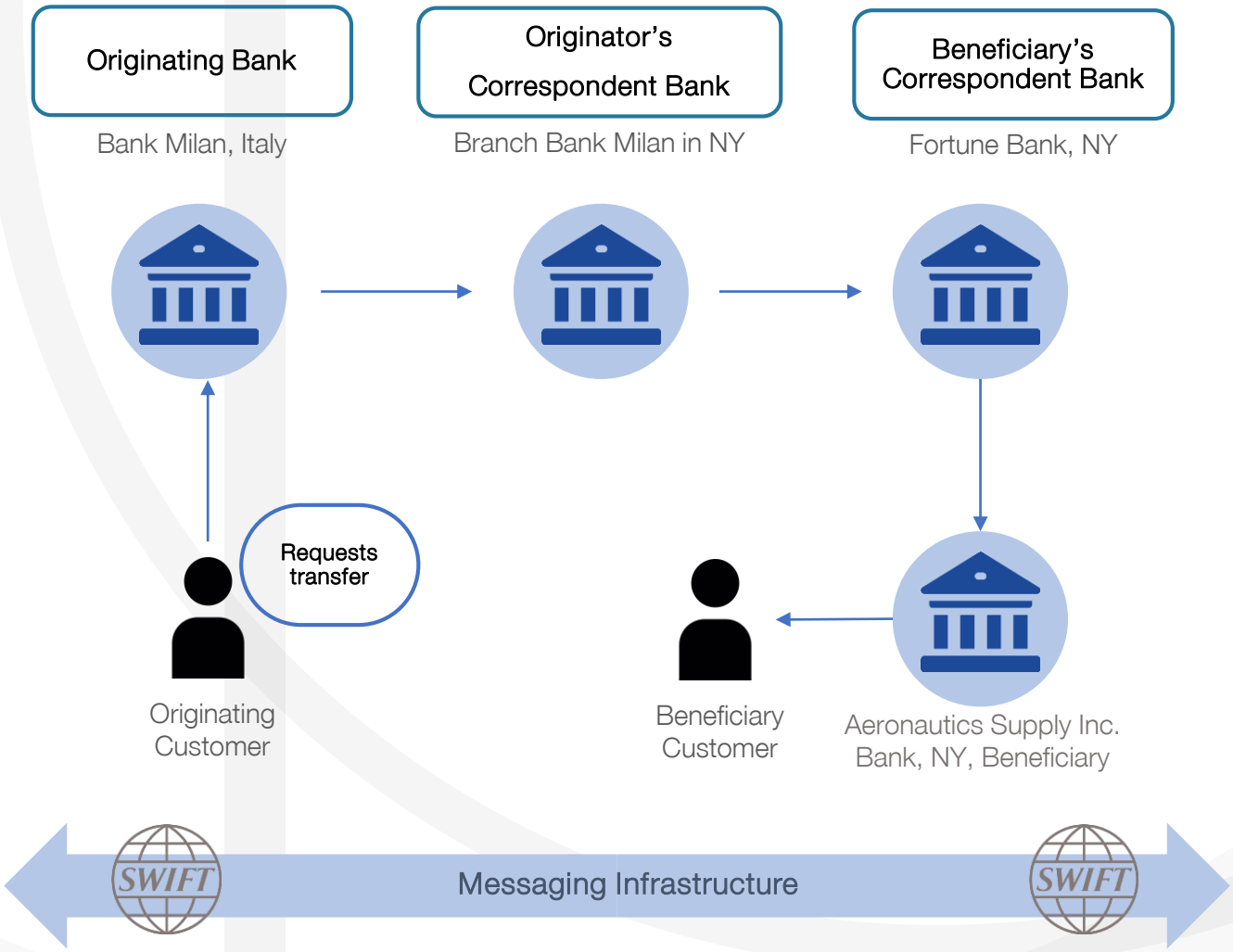
	Switzerland AMLO 02/2019	**FATF** R.16 Travel Rule	**U.S. FinCEN** Travel Rule	**Singapore** PSA
Transaction Threshold (to share data)	over 1000 CHF (from 01/2021)	FI must share data for transaction over 1000 USD or EURO	Over USD 1,000	Over $1,500 (roughly $1000)
Originator Data	• Name • Account number • Physical Address, national ID number or date and place of birth	• Name • Account number • Physical Address, national ID number or date and place of birth	• Name • Account number • Physical Address	• ID card or • Birth Certificate or • Passport or • Business certificate • date & place of birth
Beneficiary Data	• Name • Account number	• Name • Account number	• Name • Account number • Any unique identifier	• Name • Account number • Any unique identifier

2 Implementing the New Standard

From SWIFT to "Crypto SWIFT"

Providing historical context – SWIFT can be a blueprint for VASPs and VAs. The Travel Rule Protocol can be compared with SWIFT's functionality. To solve the communication cross border payments problem in 1973, banks formed a cooperative utility, the Society for Worldwide Interbank Financial Telecommunication, headquartered in Belgium.

SWIFT went live with its messaging services in 1977, replacing the Telex technology which was predominantly used to exchange messages. The main components of the original services included a messaging platform, a computer system to validate and route messages, and a set of message standards. The standards were developed to allow for a common understanding of data across linguistic and system boundaries and to permit the seamless, automated transmission, receipt, and processing of communications exchanged between users. Having disrupted the manual processes that were the norm of the past, SWIFT is now a global financial infrastructure that spans every continent, more than 200 countries and territories, and services more than 11'000 institutions around the world.



Source: FinCEN

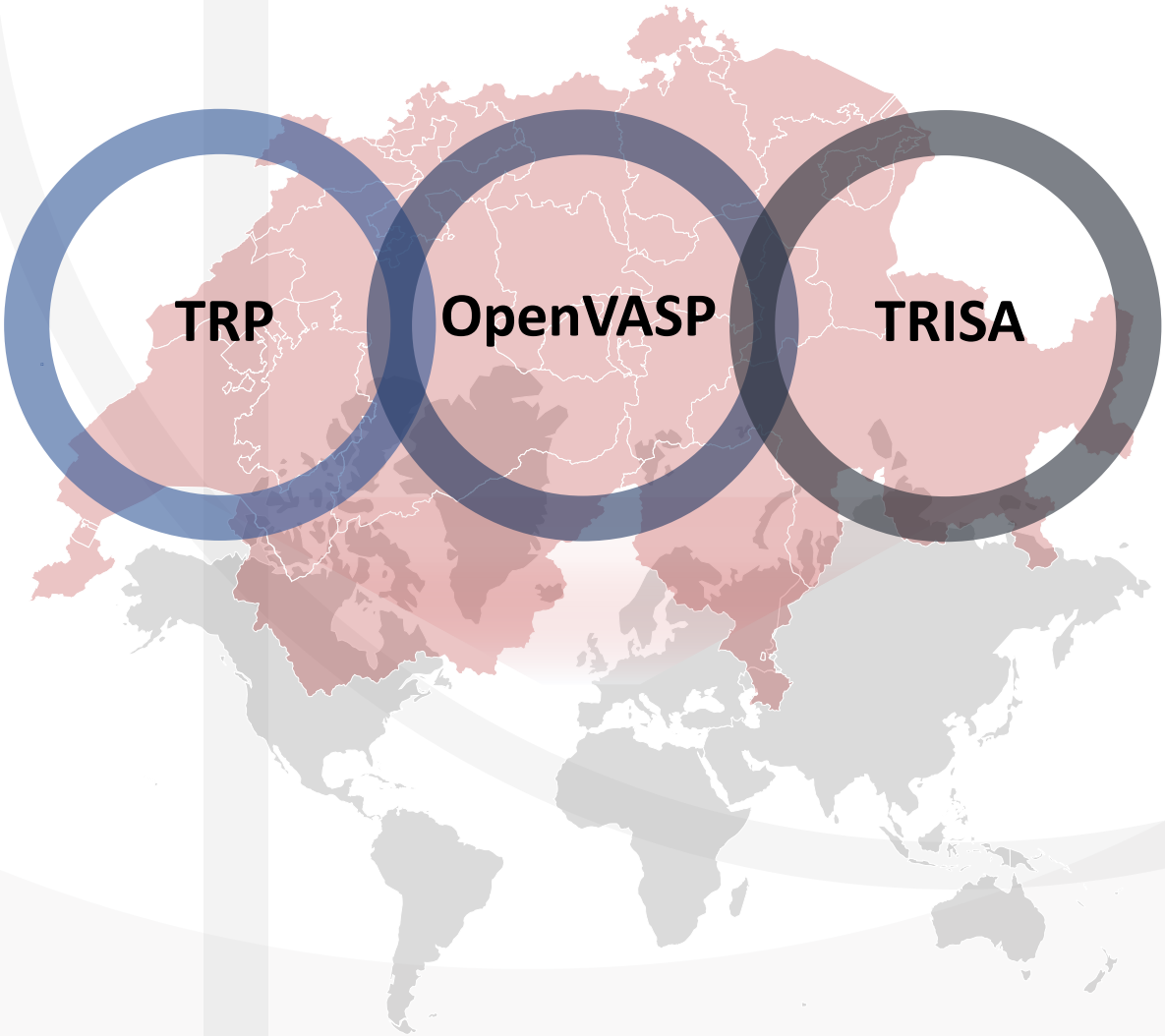
Global Overview “Protocols”

Since Summer 2019 many developers and companies have been focused on implementing a solution or protocol to accommodate closely to the FATF recommendations. In most cases there are no central bodies or organisations behind a protocol, but rather a variety of leading industry participants from around the world, who have joined together to groups that openly participate in the implementation and further development of a solution. Despite all having a similar aim to create a simple solution which will not impose unnecessary additional requirements, integrate into existing business/solutions and enable interoperability, the chosen approaches differ in its core architectural philosophy.

There are several leading developers and companies who already presented a version of their approach to the market. Whereas some of the them are still in a testing phase, others already launched. By August 2020 the first transmission between two Swiss VASP’s took place, by using the TRP implemented as a Software-Solution by the Swiss software developer 21 Analytics.

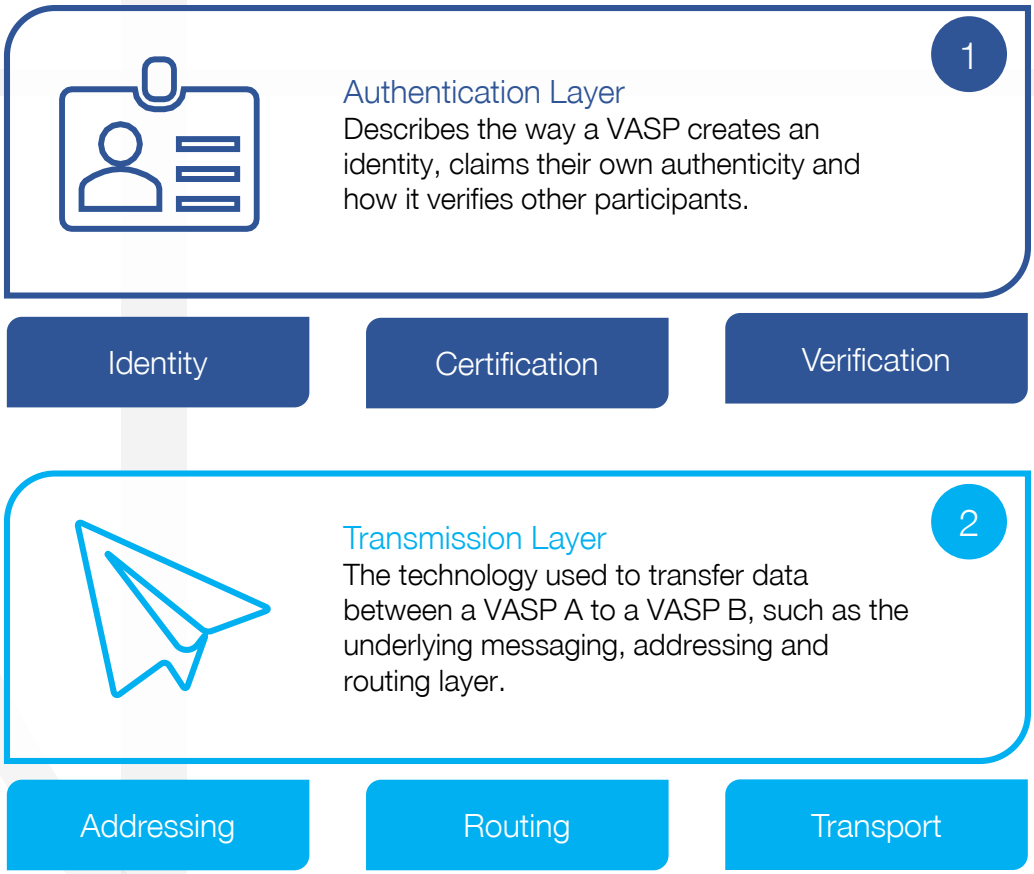
Front Runner protocols

Out of the various different implementations gwp has analysed the most prominent opensource, non-commercial Travel Rule solutions emerging foremost in the Swiss/ European market, TRP, OpenVASP and TRISA.

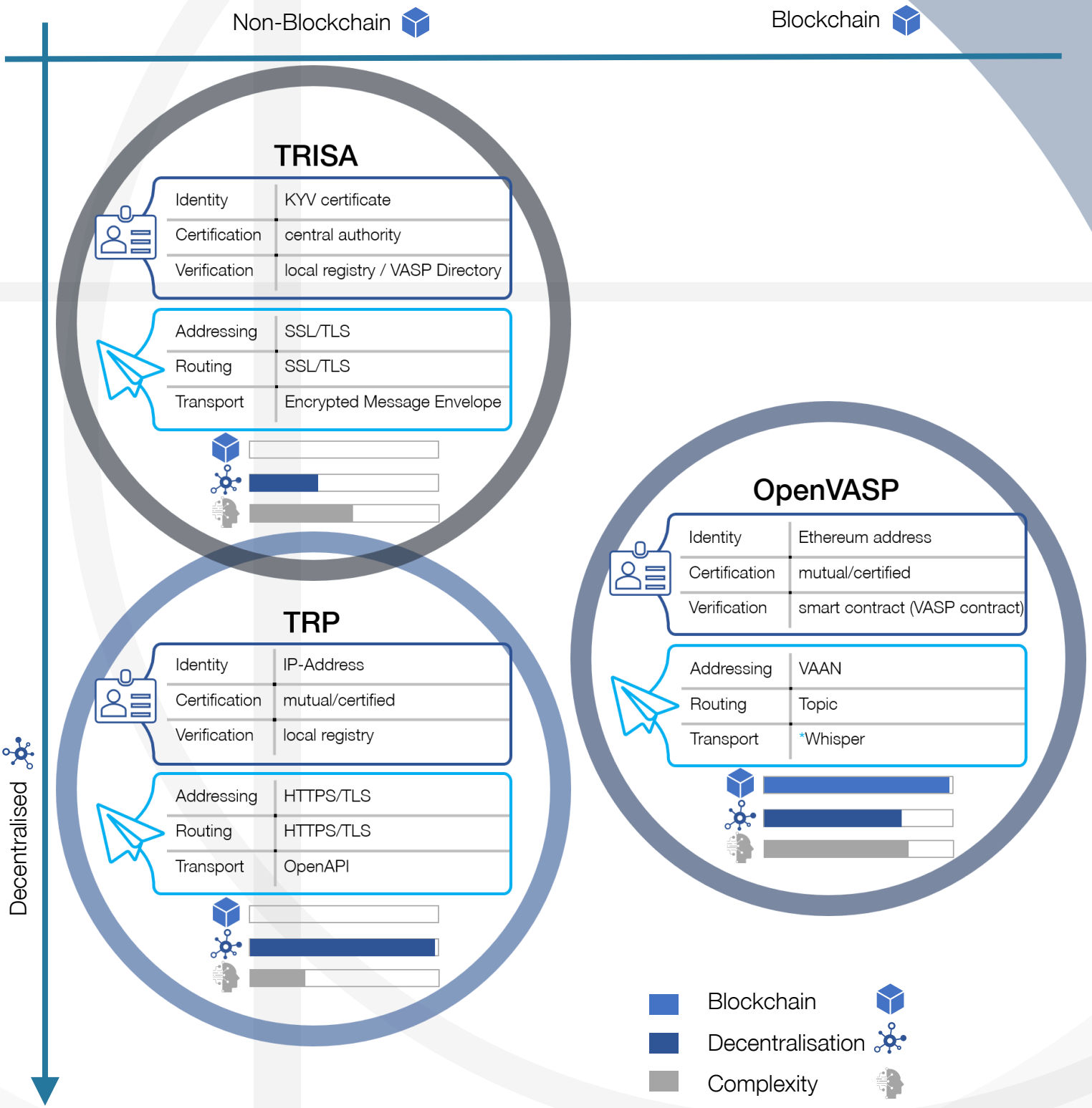


Methodology

Two critical characteristics are identified, as to be an adequate factor to compare the architecture of the protocols: authentication- and transmission-layer. Accordingly, we have focused on three aspects of each layer, with the aim to enable the reader to understand the main differences and evaluate possible implications when implementing/integrating a protocol to their own infrastructure. A detailed technical overview of each protocol is provided in this chapter.



Characteristics



*Given the minimal requirements of the OpenVASP protocol, there is a wide range of possible messaging layer which could be used. Whisper is only one example of a possible implementation..

Travel Rule Protocol (TRP)

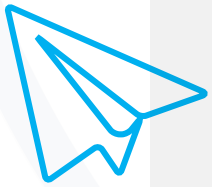
A Minimal, Pragmatic API for Compliance with FATF Travel Rule Recommendations for Virtual Assets

The project team is proposing an open, collaboratively-managed infrastructure that offers VASP members a way to comply with FATF Travel Rule recommendations for virtual assets. The project's main approach is to develop an easy to use solution, by focusing closely on the FATF recommendation, limiting the scope and trying not to impose unnecessary additional requirements to the participants. Therefore enabling any businesses or solutions to integrate with minimal friction and effort.

1

The authentication layer of the TRP is based on mutual authentication. Basically every participant maintains an own list of authenticated and therefore trusted counterparties, which ordinarily comes into existence when a business relationships are established. By having such a set up, there is no central application or database needed, instead the protocol runs within each VASP's infrastructure itself.

2

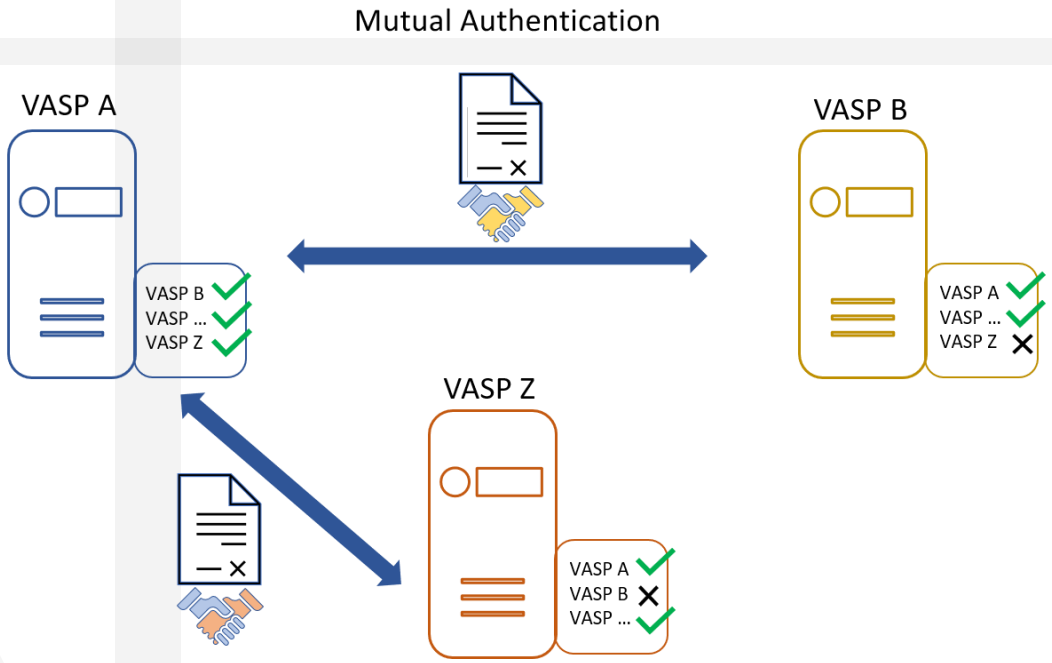


The communication layer is based on a simple set of RESTful endpoints and a minimal, workable and pragmatic API solution. The underlying messaging layer is therefore relying on the common HTTP requests to transmit the data between the two participants.

1 Authentication

Identity

The identity of a VASP using the TRP is defined by its underlying technology, which in this case is the internet protocol. As a common participant in the internet, the VASP would therefore be identified by it's IP-Address and can be reached by using the correct routing information (handshake) and authentication methods (cryptographic keys).



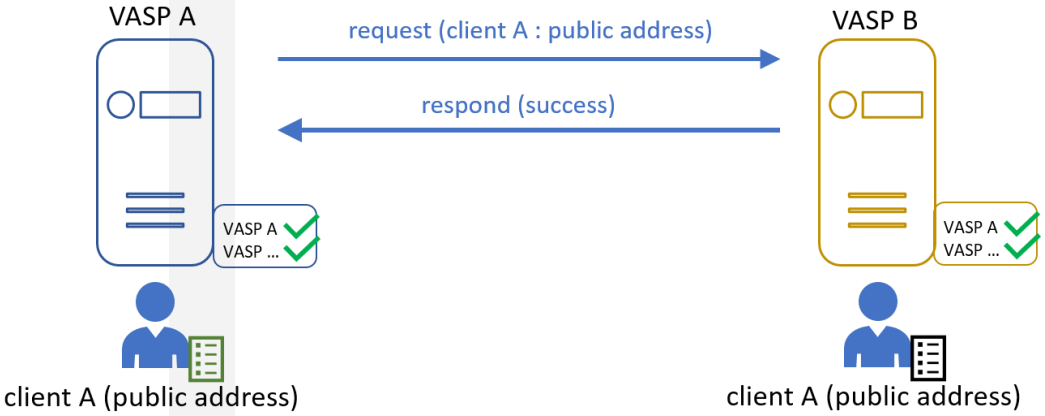
Certification/Verification

Similar to a human interaction with the Internet, when opening a website address (e.g. URL), the human must know or have searched for the address in order to connect to the website. The same applies to VASPs that attempt to transmit data to a recipient VASP. To connect to another VASP, the identity must be exchanged in advance (e.g. VASP A and VASP B), which is usually done on the basis of a mutual agreement between the VASP's during the onboarding process, but could also be provided by a certified authority. Thereafter, each VASP will maintain a list/register of known and verified VASPs, which is needed to establish a connection and make any related API calls to a respective VASP.

2 Transmission

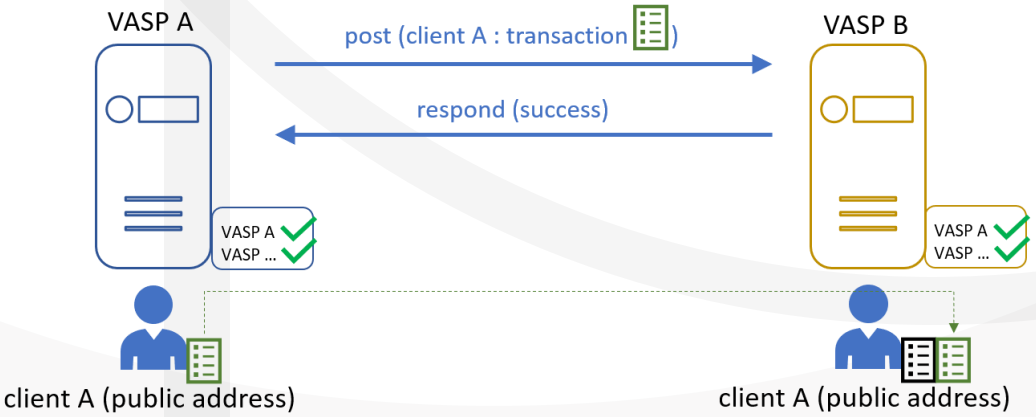
Addressing/Routing

For addressing purposes the TRP uses the information shared during the authentication of the counterparty VASP, to establish a connection between VASP A (originator) and VASP B (beneficiary). The application is an API that can be integrated with other backend system to run automatically a set of different services to create, read, update or delete data (e.g. beneficiary information regarding FATF recommendation). As soon as the connection between two VASP is established, the originating VASP A can query an address to the beneficiary VASP B. When the API is called, the beneficiary VASP will respond, depending on if the given address is know and is under management.



Transport: OpenAPI transaction notification

The OpenAPI Specification (OAS) defines a standard, language-agnostic interface to RESTful APIs which allows both humans and computers to discover and understand the capabilities of the service without access to source code, documentation or through network traffic inspection. Whenever a transaction between two VASPs occurs, the originator VASP will transmit the beneficiary information (e.g. client A) by using a POST service defined by the OpenAPI specification.



OpenVASP

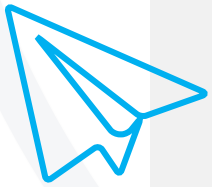
Open protocol to implement FATF's travel rule for virtual assets.

The OpenVASP protocol is driven by a "decentralised" philosophy of their developers and contributors. This is reflected in the protocol design and architecture. By leveraging some of the capabilities of the Ethereum blockchain, the protocol claims to enable cryptographically secured communication and authentication, with the goal of ensuring data privacy without the need for a central authority.

1

As an authentication layer OpenVASP uses a so called VASP contract, which represents an identity of a VASP on the decentralised public key infrastructure of Ethereum. Therefore a smart contract is deployed containing the credentials of the VASP. To establish a business relationship among VASPs the VASP identity is exchanged in a direct mutual or certified way.

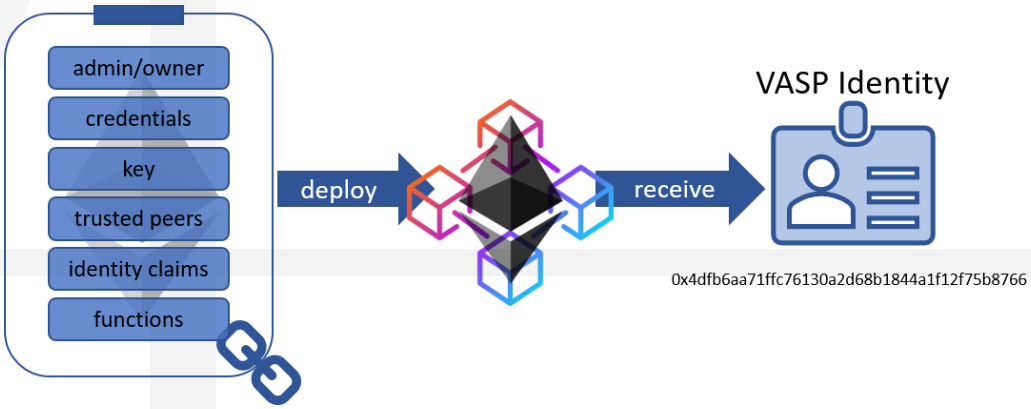
2



A *possible messaging layer is built on top of the Ethereum infrastructure by using Whisper. Whisper can be categorised as an identity-based pseudonymous low-level messaging system, which combines aspects of distributed hash tables DHTs and datagram messaging systems (e.g. UDP). One of it's core design principles are the modular privacy and anonymity features.

*Given the minimal requirements of the OpenVASP protocol, there is a wide range of possible messaging layer which could be used. Whisper is only one example of a possible implementation..

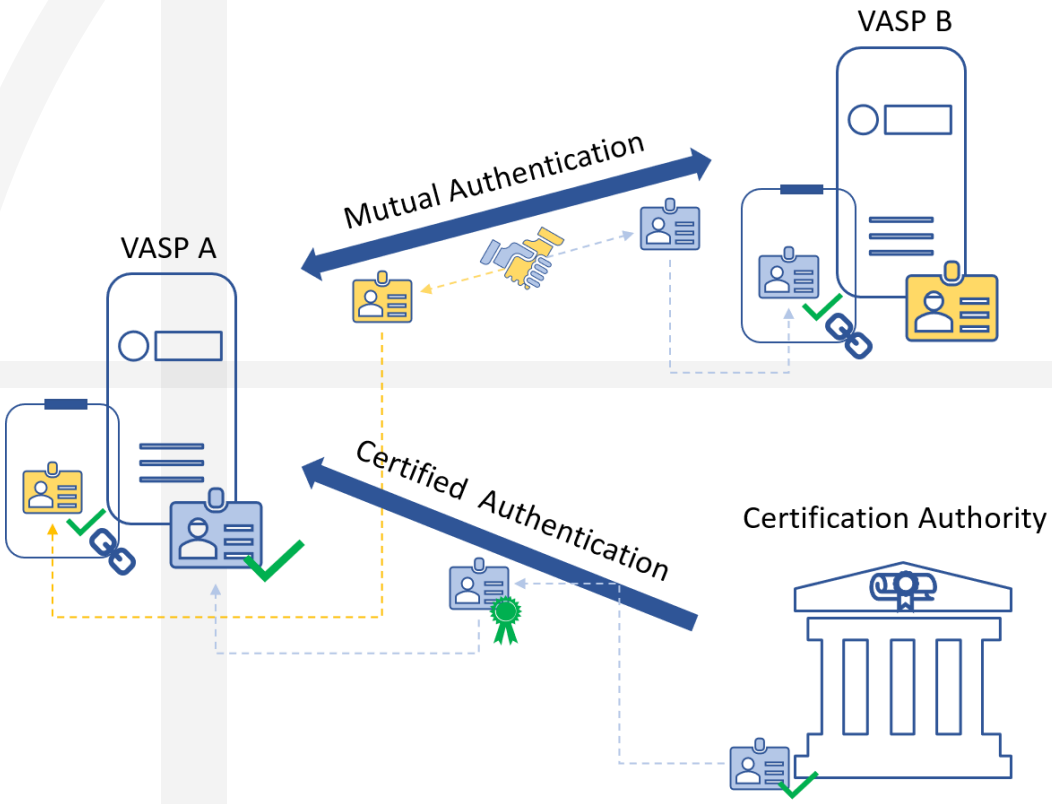
1 Authentication



Identity: VASP Contract/VASP Identity

For a VASP to use the OpenVASP protocol, one of the first steps would be to create an VASP Identity on the Ethereum blockchain. To do so, each VASP will deploy a standardised smart contract, containing the VASP's credentials (simplified in picture above), cryptographic keys (handshake and signing), admin/owner specifications (to manage the smart contract) and a set of functions, used to manage trusted peers or to claim an identity from a third party. By deploying the smart contract you will receive automatically an Ethereum contract address which is defined to be the VASP identity.

1 Authentication



Certification/Verification

Since the deployment of a smart contract is open to everyone, the possession of a VASP identity itself is not a guarantee for the authenticity of the VASP. The OpenVASP protocol considers two different approaches to authenticate among VASPs.

Mutual Authentication

Whenever two VASPs establish a business relationship, their respective identities can be directly authenticated, i.e. there is first-hand evidence that the identity of the other VASP is genuine. Hence, the VASP A will add VASP B's identity as a trusted VASP to their smart contract.

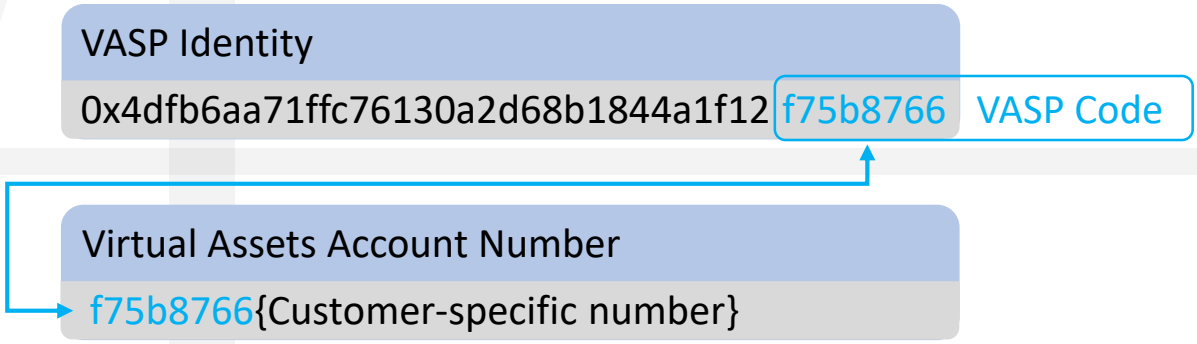
Certified Authentication

The certified authentication approach relies on a Trusted Third Party, which can be compared to a current certification authority to issue digital signature or Secure Socket Layer (SSL) certificates. VASP A therefore needs to claim an identity with a certification authority. Such certification authorities could include a certificate of the license or registration status of the VASP issued by the relevant authorities. The OpenVASP Directory is meant to act as such a certification authority.

2 Transmission

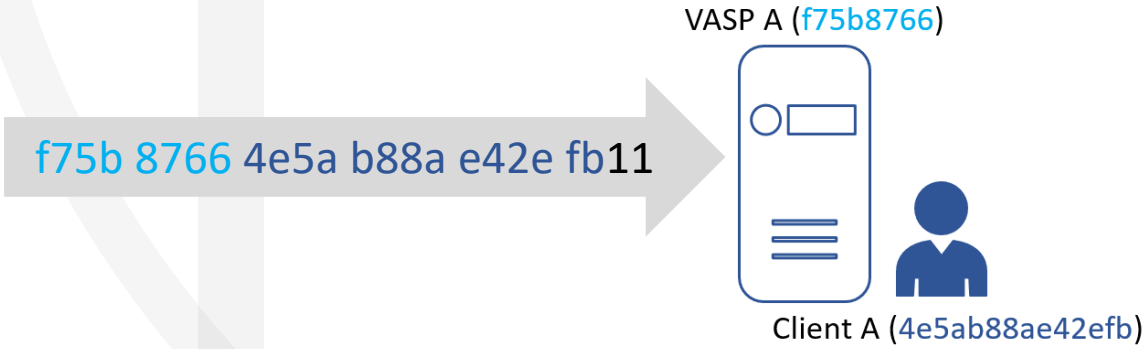
Addressing: VASP code and Virtual Assets Account Number (VAAN)

The OpenVASP protocol makes use of the VASP Identity address to create a unique VASP code and the Virtual Assets Account Number (VAAN). Whereas the VASP Code is defined by the last 32 bits of the VASP identity address, the VAAN is a combination of the VASP Code and a customer specific number of 56 bits.



Routing information

The routing information is used to declare the recipient's address. The traditional banking system makes use of common standards as BIC/SWIFT or IBAN , which represent a combination of a bank identifier and a respective account number. Similar to these approaches the VAAN number includes a VASP identifier (VASP-Code) and the recipient's address (customer-specific number e.g. 4e5ab88ae42efb).



Transport: Whisper

As soon as the receiving VASP and the client are identified and the respective authentication measures have been carried out, the last step of the protocol is to transmit the data as defined by the FATF Travel Rule among the VASPs. On a high-level the Whisper messaging layer uses asymmetric or symmetric encryption, to encrypt a message, which therefore can only be decrypted by it's defined recipient. Although the message is sent to a decentralised network, meaning it will be received by multiple participants (nodes), only the defined recipient will be able to decrypt the message and unveil the content, resulting in providing anonymity for the recipient. To avoid unnecessary computational resources to decrypt all incoming messages, Whisper includes a 4-byte "topic" which is a probabilistic hint for the recipient to watch out for a message and try to decrypt. The OpenVASP protocol benefits from the previously explained address format VAAN by using the VASP-Code as topic, resulting in less computational resources and a faster transmission in the network.

Travel Rule Information Sharing Architecture (TRISA)

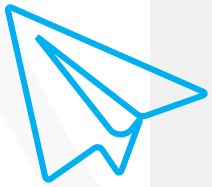
Critical Infrastructure to Address Interoperability Issues Presented by the FATF's Travel Rule Requirements

The goal of TRISA is to enable compliance with the Travel Rule without modifying the core blockchain protocols and having an open governance body. Thereby, their focus is on an open source and decentralised approach, considering and maintaining interoperability with other approaches. The protocol proposes a peer-to-peer mechanism, with minimal cost impact to participants, preserving high performance transactions and protecting user privacy.

1

The main authentication layer in the TRISA protocol follows a certificate authority (CA) model. It is understood as an authority that issues so called public key certificates, which are maintained in a central directory. This certificate represents the VASP's identity and is used to establish a secure communication between VASPs. For a VASP to obtain such a certificate it has to go through a registration process, including the verification of their identity.

2

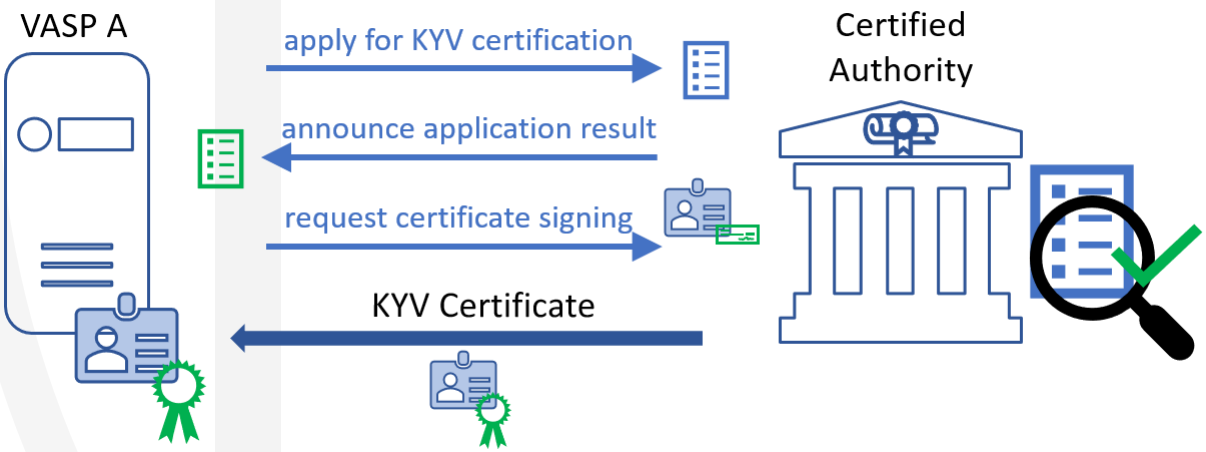


To establish a secure transmission channel between two VASPs, the TRISA protocol uses a mutually authenticated SSL/TLS connection. This ensures the privacy of data in the transition phase and enables to keep a connection open for multiple transactions over a single peer-to-peer connection. Further TRISA is proposing an encrypted message format, to keep the data accessible at any time in case further checking is necessary (e.g. financial investigation, SAR filing).

1 Authentication

Identity & Certification: Know Your VASP

The registration process called “Know Your VASP” is designed to fulfill and verify all legal requirements of any applying VASP. For this purpose a VASP A must submit a certification request with all relevant business credentials to a registered certification authority in order to obtain a “Know Your VASP Certificate”, the identity of the VASP A. The data is then checked against a number of criteria, such as their business registration, KYC check, jurisdiction, fraud and sanctions and, if necessary, also against other extended validation criteria. If all requirements have been met, the certificate authority will sign the certificate signing request from the applying VASP A and issues the Know Your VASP Certificate.



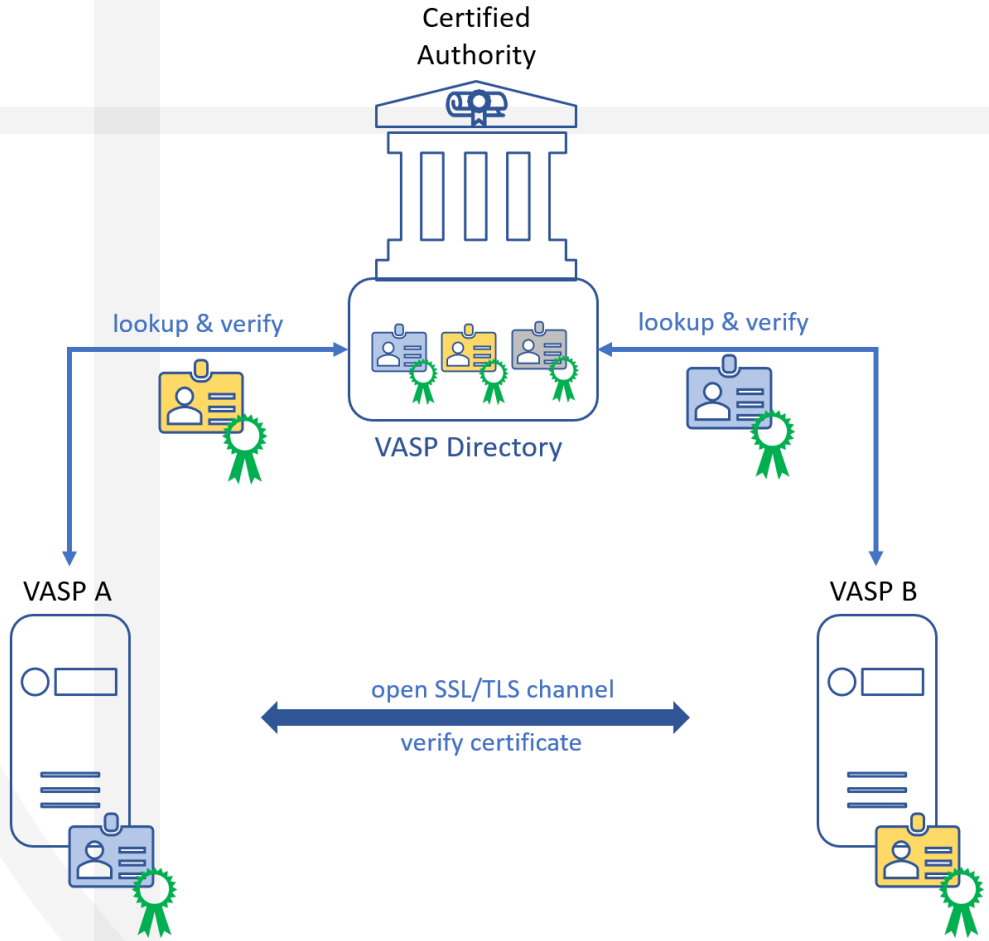
Verification: TRISA VASP Directory

TRISA operates a hosted certificate authority, which maintains a VASP Directory of all registered VASPs. As means of verification, as soon as a VASP A want’s to connect to a VASP B, it can simply check for the Know Your VASP B’s certificate or lookup the business credentials in the VASP directory, considering that the beneficiary VASP B is a legitimate participant compliant to the Know Your VASP requirements. This has the advantage of allowing a VASP to make an informed compliance decision before sending or receiving a virtual asset transaction.

2 Transmission

Addressing & Routing

Based on the Know your VASP certificate issued by a certified authority, the addressing works by a mutual authentication between the VASP A and VASP B. Basically, this involves only the exchange of the VASP identity (public address). In fact, holding a counterparties identity guarantees it's authentication, and is therefore enough to open a secure SLL/TLS channel, used to exchange information, while still protect user privacy. Thus being a direct peer-to-peer connection, no further routing information is needed.



Transport

The presented SSL/TLS channel to send cryptographically secured private information, would satisfy the requirements of the FATF concerning data privacy and security. To enhance the data handling, TRISA proposed to use an additional encryption on the transport layer, an encrypted transaction envelope. By adding this additional layer consisting of an encryption key and HMAC key, VASPs can securely store the full transaction data independent of their used backend, while maintaining the full reproducibility.

3 Glossary & Sources

Glossary

- AML/CFT obligation or purpose: The Act imposes several obligations if you operate a business that falls within the definition of a reporting entity
- AMLO-FINMA: Swiss Federal Act on Combating Money Laundering and Terrorist Financing.
- dApps: Decentralised applications (dApps) are digital applications or programs that exist and run on a blockchain or P2P network of computers instead of a single computer, and are outside the control of a single authority.
- DeFi: The term DeFi stands for “decentralised finance” and is usually used to describe the cluster of applications and companies offering financial services based on decentralised blockchain technology.
- DHT: Distributed Hash Table refer to a distributed system that provides a lookup service to retrieve a value by using an associated key (key-value pairs).
- FATF 12-month review: a 12-month review to measure the implementation of the revised standards by jurisdictions and the private sector, as well as monitoring for any changes in the typologies, risks and the market structure of the virtual assets sector.
- FATF Blacklist Countries (High-Risk Jurisdictions): Democratic People's Republic of Korea, Iran
- FATF Member Countries: Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Co-operation Council, Hong Kong, China, Iceland, India, Ireland, Israel, Italy, Japan, Republic of Korea , Luxembourg, Malaysia, Mexico, Netherlands, Kingdom of, New Zealand, Norway, Portugal, Russian Federation, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States
- FATF: Financial Action Task Force, an intergovernmental organisation that develops policies to Combat Money Laundering and Terrorist Financing
- FCA: Financial Conduct Authority, the financial regulatory body of the UK
- Financial Intermediary (FI): refers to a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution
- FinCEN: Financial Crimes Enforcement Network, the United States federal bureau that analyses information about financial transactions in order to fight Money Laundering, terrorist financing, and other financial crimes
- FINMA: The Swiss Financial Market Supervisory Authority (FINMA) is the Swiss government body responsible for financial regulation. This includes the supervision of banks, insurance companies, stock exchanges and securities dealers, as well as other financial intermediaries in Switzerland.
- HMAC key: HMAC (sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key.
- MAS Payment Service Act 2019: The Payment Services (PS) Act is a forward looking and flexible framework for the regulation of payment systems and payment service providers in Singapore. It provides for regulatory certainty and consumer safeguards, while encouraging innovation and growth of payment services and FinTech. Parliament passed the PS Act on 14 January 2019.
- ML/TF risk: customer risk is the risk or vulnerability that customers may be involved in Money Laundering or Terrorist Financing activities. ML/TF customer risk is significantly influenced by the nature and/or attributes of a customer.
- OpenVASP: an open protocol to implement the travel rule that includes all names: Bitcoin Suisse AG|Lykke | SEBA Bank AG | Sygnum Bank AG | MME Legal Tx Compliance | Avaloq Evolution AG | EPAM Systems, Inc.| 21 Analytics AG | Notabene, Inc. | Web3 Foundation | Coinfirm | Tezos Foundation | TRM Labs | Netki, Inc. | Merkle Science

Glossary

- P2P: Stands for “peer to peer." In a P2P network, the "peers" are computer systems which are connected to each other via the internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.
- Risk Based Approach: A risk-based approach means that countries, competent authorities, and banks identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk.
- SSL/TLS channel: Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL) are cryptographic protocols designed to provide communications security over a computer network.
- SWIFT: The Society for Worldwide Interbank Financial Telecommunication (SWIFT), legally S.W.I.F.T. SCRL, provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardised and reliable environment.
- Travel Rule: A Bank Secrecy Act (BSA) rule [31 CFR 103.33(g)]—often called the “Travel” Rule—requires all financial institutions to pass on certain information to the next financial institution, in certain funds transmittals involving more than one financial institution.
- TRISA an open protocol to implement the travel rule that includes all names : CipherTrace | Ripple | Paxful | MIT Connection Science ¬ Engineering | Bradley Arant Boult Cummings LLP | Luminous Group Limited.
- TRP an open protocol to implement the travel rule that includes all names : 21 Analytics | AGA&D ForensicsBC Group | OSL | BitGo | CipherTrace |Complifact AML Inc. | Crypto Finance AG | Diginex/EQUOS.io | Electric Coin Company | Elliptic | Digivault | Fidelity Digital Assets | Geissbühler Weber & Partner (gwp) | HashKey | Hex Trust | Hodlnaut Pte. Ltd. | ING | Komainu (Jersey) Limited | KPMG Advisory | KYC-Chain | Metaco | MIT Connection Science & Engineering | Netki | Notabene | OKCoin | Onchain Custodian | Ospree | Paxful | Peter Davey and Associates Limited | Standard Chartered Bank | TP ICAP | Trisa | Xreg.
- Unhosted wallets: are software hosted on a person's computer, phone or other device that allow the person to store and conduct transactions in crypto assets.
- UDP: User Datagram Protocol is a minimal, connectionless network protocol, which is used as transport layer in the Internet Protocol, to send messages (datagrams) to other hosts.
- VA: Virtual Assets.
- VAAN: Virtual Assets Account Number.
- VASP: Virtual Asset Service Providers, who are custodial entities that run fiat-to-crypto or crypto-to-crypto exchanges, or run businesses related to transfer and safekeeping of virtual - assets and financial services.

Sources

Admin.ch. 1997. Federal Act On Combating Money Laundering And Terrorist Financing. [online] Available at: <https://www.admin.ch/opc/en/classified-compilation/19970427/202002180000/955.0.pdf> [Accessed 21 September 2020].

Bryant, A., 2019. Using Instant Messenger To Explain The FATF Travel Rule For Vasps — Andy Bryant. [online] andybryant.me. Available at: <https://www.andybryant.me/blog/2019/9/25/using-instant-messenger-to-explain-the-fatf-travel-rule-fornbspvasps> [Accessed 23 September 2020].

Docs.google.com. 2020. *Travel Rule Protocol 20200617*. [online] Available at: <https://docs.google.com/document/u/0/d/1UubLDy9rlvUfS4WxkLjWiQxM-2KP_GrRdCh5PzwilTM/mobilebasic> [Accessed 17 September 2020].

Eidgenössische Finanzmarktaufsicht FINMA. 2020. *FINMA Guidance 02/2019*. [online] Available at: <https://www.finma.ch/en/documentation/finma-guidance/> [Accessed 17 September 2020].

Ethereum Wiki. n.d. *Whisper Poc 2 Protocol Spec*. [online] Available at: <https://eth.wiki/en/concepts/whisper/poc-2-protocol-spec> [Accessed 17 September 2020].

Fatf-gafi.org. 2020. 12-MONTH REVIEW OF THE REVISED FATF STANDARDS ON VIRTUAL ASSETS AND VIRTUAL ASEET SERVICE PROVIDERS. [online] Available at: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf> [Accessed 23 September 2020].

Fatf-gafi.org. 2019. VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS. [online] Available at: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf> [Accessed 21 September 2020].

Fatf-gafi.org. 2020. *Outcomes FATF Virtual Plenary, 24 June 2020*. [online] Available at: <https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-fatf-plenary-june-2020.html> [Accessed 17 September 2020].

Fatf-gafi.org. 2020. *What We Do - Financial Action Task Force (FATF)*. [online] Available at: <https://www.fatf-gafi.org/about/whatwedo/> [Accessed 17 September 2020].

Fincen.gov. 2020. *Fincen Advisory*. [online] Available at: <https://www.fincen.gov/sites/default/files/advisory/advissu7.pdf> [Accessed 17 September 2020].

Jevans, D., 2019. *Travel Rule Information Sharing Architecturefor Virtual Asset Service Providers (TRISA)*. [online] Linkedin.com. Available at: <https://www.linkedin.com/pulse/travel-rule-information-sharing-architecture-virtual-asset-jevans> [Accessed 17 September 2020].

Kirkpatrick, K., Telep, J., Das, S. and Gerber, J., 2020. *Fincen 'Travel Rule' Update Sets Challenges For Crypto Cos.*. [online] Kslaw.com. Available at: <https://www.kslaw.com/attachments/000/007/286/original/FinCEN_'Travel_Rule'_Update_Sets_Challenges_For_Crypto_Cos..pdf?1571236052 > [Accessed 17 September 2020].

KYC-Chain. 2020. *How The FATF's Travel Rule Is Being Implemented Around The World - KYC-Chain*. [online] Available at: <https://kyc-chain.com/fatf-travel-rule-around-the-world/> [Accessed 17 September 2020].

Riegelnig, D., 2019. *Openvasp: An Open Protocol To Implement FATF'S Travel Rule For Virtual Assets*. [online] Openvasp.org. Available at: <https://openvasp.org/wp-content/uploads/2019/11/OpenVasp_Whitepaper.pdf> [Accessed 17 September 2020].

Swagger.io. 2020. *Openapi Specification - Version 3.0.3 | Swagger*. [online] Available at: <https://swagger.io/specification/> [Accessed 17 September 2020].

Switzerland, F., 2020. *Swiss 21 Analytics Completes First Automated And Compliant Bitcoin Transaction | Fintech Schweiz Digital Finance News - Fintechnewsch*. [online] Fintech Schweiz Digital Finance News - FintechNewsCH. Available at: <https://fintechnews.ch/blockchain_bitcoin/swiss-financial-intermediaries-successfully-complete-first-automated-and-compliant-bitcoin-transaction/38328/> [Accessed 17 September 2020].

Sygna. 2020. FATF Announces New 12-Month "Travel Rule" Review For June 2021 - Sygna. [online] Available at: <https://www.sygna.io/blog/fatf-plenary-new-travel-rule-12-month-review-for-june-2021/> [Accessed 23 September 2020].

Sygna. n.d. Singapore Crypto Regulation: A Licensing Guide For DPT Exchanges - Sygna. [online] Available at: <https://www.sygna.io/blog/singapore-cryptocurrency-regulations-and-digital-payment-token-service-licensing/> [Accessed 21 September 2020].

Sygna. 2020. *What FATF R.16 Crypto Travel Rule Solutions Are Currently In The Market? - Sygna*. [online] Available at: <https://www.sygna.io/blog/types-of-fatf-r16-crypto-travel-rule-solutions/> [Accessed 17 September 2020].

Trisa.io. 2020. *Travel Rule Information Sharing Architecture For Virtual Asset Service Providers*. [online] Available at: <https://trisa.io/trisa-whitepaper/#_Toc48780351> [Accessed 17 September 2020].

Unchained Podcast. 2020. *Why The Travel Rule Is One Of The Most Significant Regulations In Crypto - Unchained Podcast*. [online] Available at: <https://unchainedpodcast.com/why-the-travel-rule-is-one-of-the-most-significant-regulations-in-crypto/> [Accessed 17 September 2020].

Photo credits

Shutterstock, Unsplash, Pixabay

Michael Baumgartner
Head Sales Transaction Banking & Digital Assets
michael.baumgartner@incorebank.ch
+41 44 403 93 20

incore

Laragh Welti
Head Marketing
laragh.welti@incorebank.ch
+41 44 403 93 19

Ekaterina Anthony
Senior Manager, Team Leader Crypto
ekaterina.anthony@gwp.ch
+41 76 582 09 74

Jeff Borisov
DLT/Digitalisation Consultant
jeff.borisov@gwp.ch
+41 44 221 91 61

Sandro Muccione
DLT/Digitalisation Consultant
sandro.muccione@gwp.ch
+41 44 221 91 28

gwp
geissbühler weber & partner

Dianastrasse 9
8002 Zürich

+41 44 221 91 00
info@gwp.ch | www.gwp.ch