Transacting with Self-hosted Wallets as a Swiss VASP

21 ANALYTICS

MME

February 2024

Travel Rule

More than 4 years after the Financial Action Task Force (FATF) extended anti-money laundering and countering of terrorism financing (AML/CTF) to virtual assets (VAs), only 35 jurisdictions have passed the so-called Travel Rule. After the FATF advised its members to extend their activities to VAs and virtual asset service providers (VASPs) in 2019, Switzerland was one of the first jurisdictions to clarify the applicable requirements through the Swiss Financial Market Supervisory Authority (FINMA).

In order to assess the risk of a transfer of funds and to comply with anti-money laundering regulations, a VASP needs to exchange accurate information about the originator and beneficiary of transfers of funds - the so-called "Travel Rule".

Although the FATF does not strictly mandate such originator and beneficiary information to be collected in transfers between VASPs and self-hosted wallets, various countries include the requirement under their regulation. Otherwise, a loophole may weaken the effectiveness of the Travel Rule and permit transactions, in fact, between VASPs to go unidentified through self-hosted wallets.

Transacting with self-hosted wallets

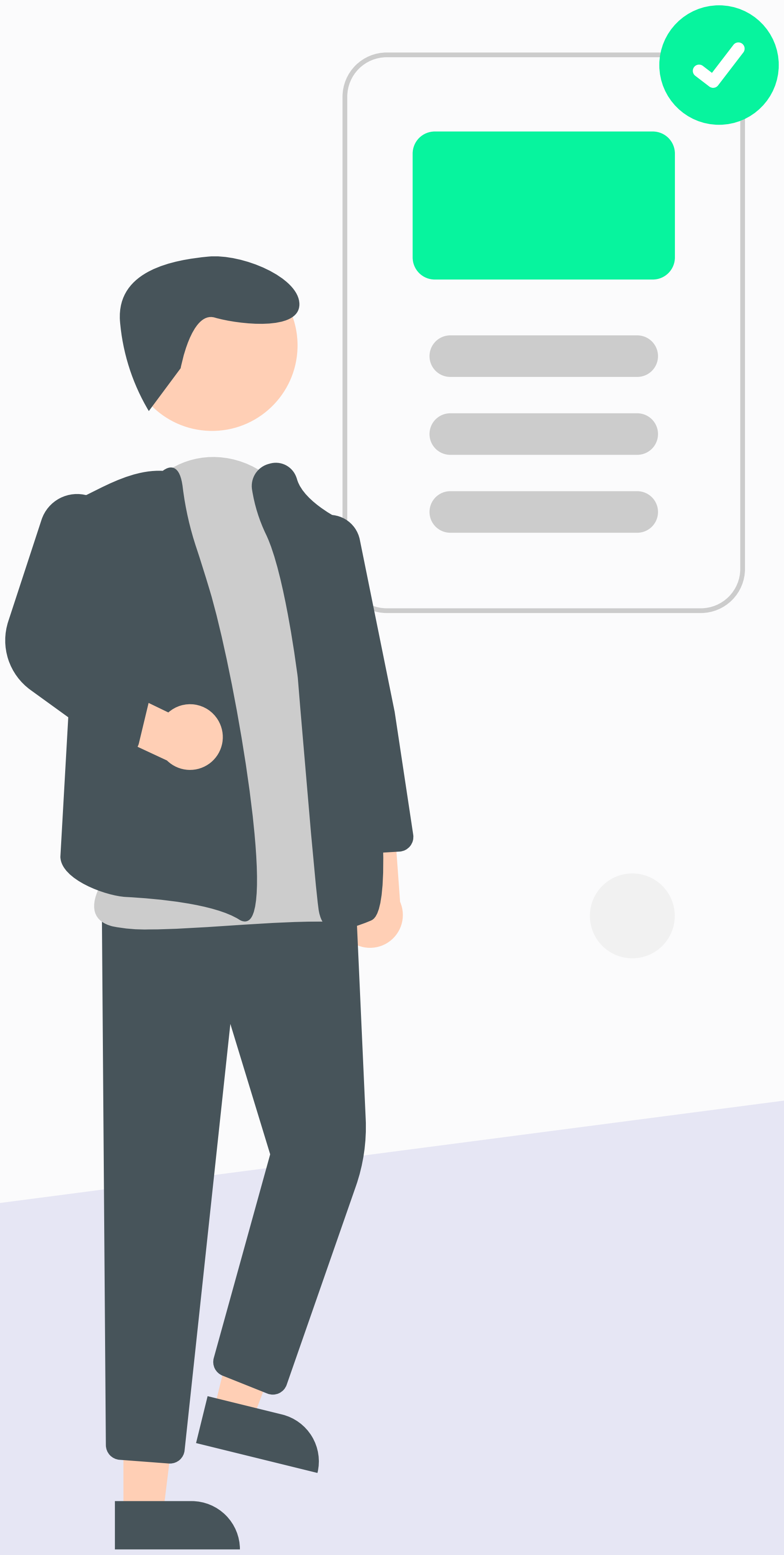
FINMA's clarity on the topic was brought by its Guidance 02/2019, mandating Swiss VASPs to identify the beneficial owner of all external wallets or addresses, in the same manner as their own clients, prior to engaging in any VA transaction or exchange. Specifically:

- for transfers to/from an external private wallet (i.e. self-hosted, non-custodial, private) belonging to an existing onboarded client, a VASP must verify that the client has the ownership of his/her external private wallets by using "suitable technical means"; or

- for transfers to/from an external private wallet belonging to an external third party (not an existing client), the VASP must (a) verify the identity of the third party, (b) establish the identity of the beneficial owner, and (c) prove the third party's ownership of the external wallet by using suitable technical means.

Concretely, this means that if John (who has an account with a Swiss VASP) wishes to transfer CHF 100 to his brother Bob (who owns a self-hosted wallet) to repay him for the birthday gift they jointly gave their mother, John's VASP will be required to validate Bob's identity and prove that he owns and controls (i.e. has the power of disposal) over his wallet.

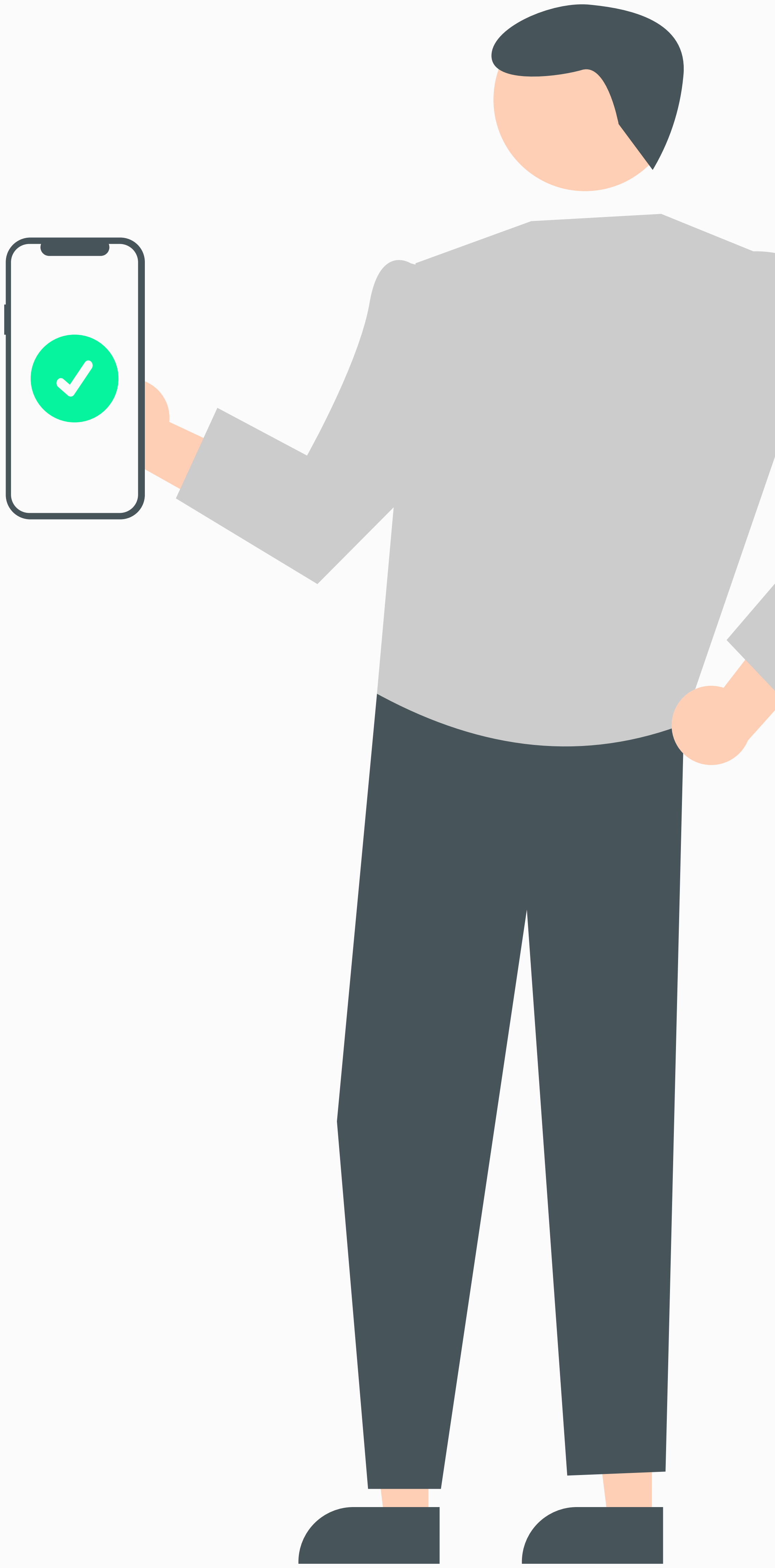
The technical means used to prove that an individual is the owner of a wallet are not defined by FINMA. Therefore, Swiss VASPs have been using distinct ways, with varying degrees of reliability and ease of user experience. This paper aims to clarify which methods are available, how they are performed and what to consider when opting for each one.



Self-hosted Wallet Ownership Proofs: Methods to Request From Customers

The VASP's goal is to have some kind of register that a person whose identity has been verified, usually their customer, has control over a specific wallet address. Only then can the VASP compliantly transact with such address, considering it whitelisted and of known ownership.

To collect an ownership proof, VASPs usually request their customers to perform one of the following methods before or at the moment of their transaction requests.



Visual Proof

A visual proof is either a screenshot or a video clip, preferably showing the customer's name, face, or document, accompanied by the current date and the wallet address to be whitelisted. In Circular 2016/7, FINMA published guidelines on video and online identification. Let's imagine David, a VASP user, is requested to provide a visual proof. David takes a screenshot displaying his face, ID, today's date, and the wallet address. He shares this image via the VASP's platform for compliance review.

VASPs may require such proof to be performed and shared through their user interface or support channels. After that, a member of the compliance team will manually review the proof to whitelist the address and, ultimately, approve the transaction.

Visual proofs are the easiest wallet verification methods to be performed by customers as they are familiar with screenshots and video tools; however, they can also be the least reliable and most susceptible to being forged, as images and videos can easily be edited.

Satoshi Test

A satoshi test consists of an agreed transaction between the customer's self-hosted wallet and VASP, performed before the customer's desired transfer in order to whitelist his/her wallet address.

A VASP will define a small, and often random, amount of cryptocurrency, a timeframe and a destination address. These details are then shared, through the VASP's user interface or support channels, with the customer who must send that amount from his/her self-hosted wallet to the destination address within that timeframe. Once the VASP identifies, in an automated or manual way, that the transaction has been received, the customer has successfully proven he/she controls the self-hosted wallet, now whitelisted to engage with the VASP.

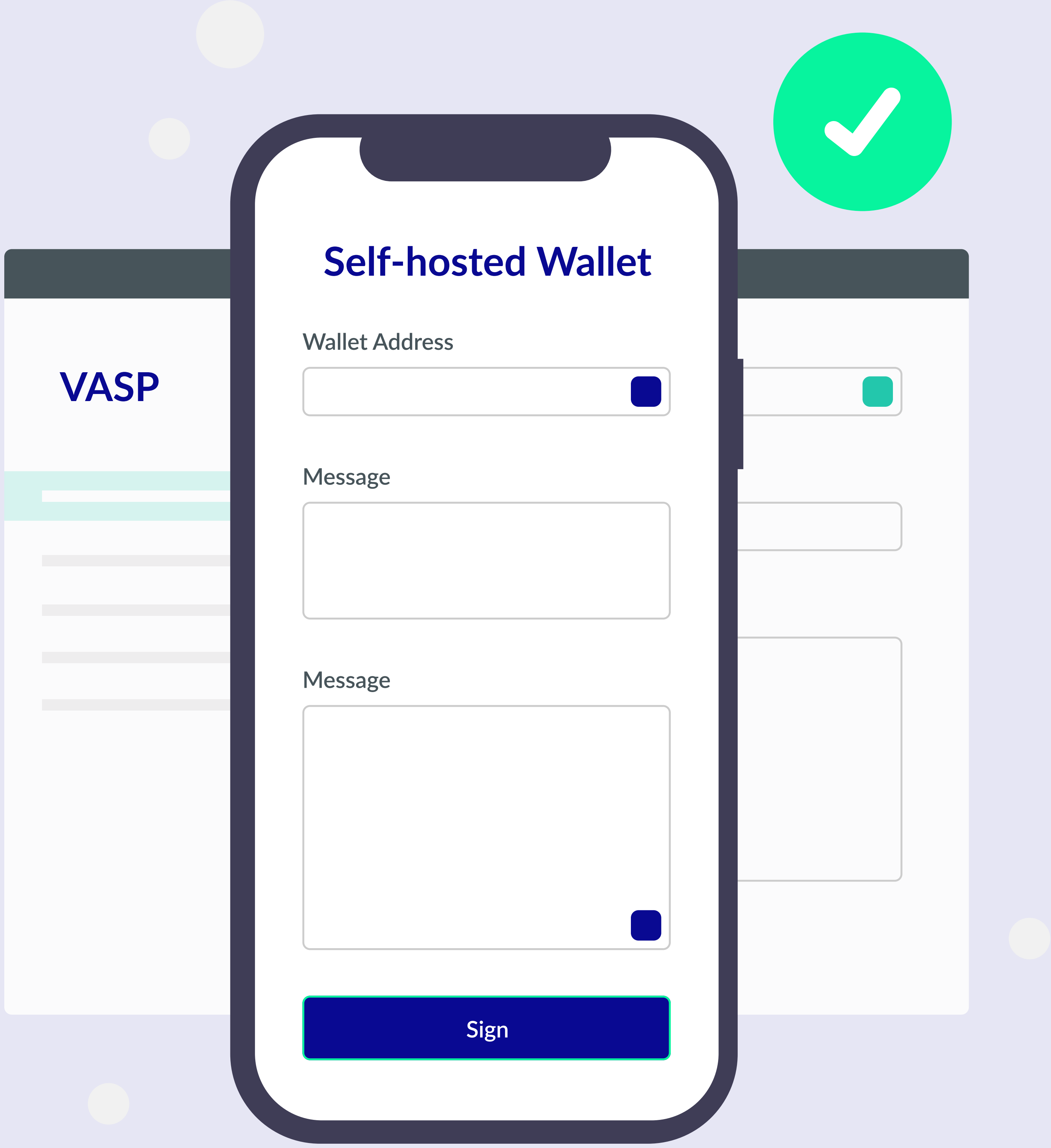
A Satoshi Test is a reliable way to tie an onboarded customer to a wallet address, but is an extensive task that interrupts the user's journey. It is not only a cumbersome process for the customer, but also for the VASP's compliance team, which needs to communicate with customers and manage their timeframes. For example, the user John, intends to transfer cryptocurrency from his personal wallet to an exchange. To ensure the security and legitimacy of his wallet, John completes a Satoshi Test by sending a small predetermined amount to the provided destination address within a specified time window.

Cryptographically Signed Message (Manual Signing)

Leveraging a feature of every self-hosted wallet, a VASP can request their customer to cryptographically sign a specific message with their private key on their wallet. The customer then shares the signature with the VASP. With the details on hand, the VASP can, automatically or manually, verify that the signature matches the message and the public key, proving the customer controls the wallet's private key. For example, let's consider Sarah, who is using a self-hosted wallet and needs to verify ownership. Upon the VASP's request, Sarah signs a personalised message containing her user identification with her wallet's private key to confirm control over her address.

The content of the message can be customised to include the details the VASP prefers, usually including the customer's name or user identification. However, the most important for the VASP is the customer's signature, which must be stored as proof that he/she controls the wallet address and reason for its whitelisting.

Although this method is reliable, as it would be rare for someone other than the wallet owner to have its private key, it is not easy for customers to perform it. The manual signing functionality is often hidden behind settings and different namings, and not all wallets show it to the end user, resulting in frustrated customers with interrupted journeys.



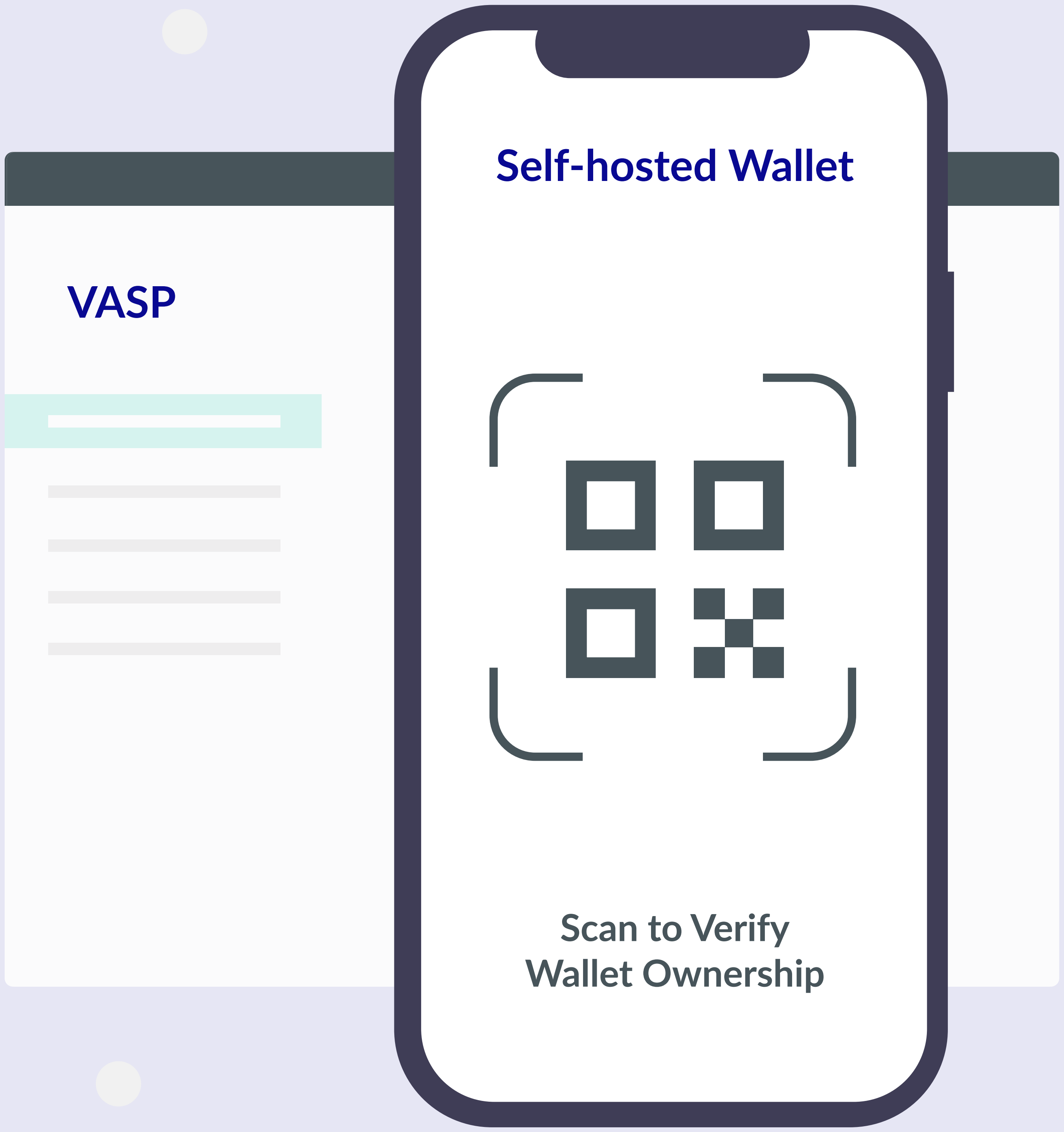
Address Ownership Proof Protocol (AOPP)

AOPP provides the same level of reliability while offering a great user experience. This is the only method that allows the customer to seamlessly continue with their transaction journey, whitelisting the address immediately, with no further delay or manual action required from the VASP.

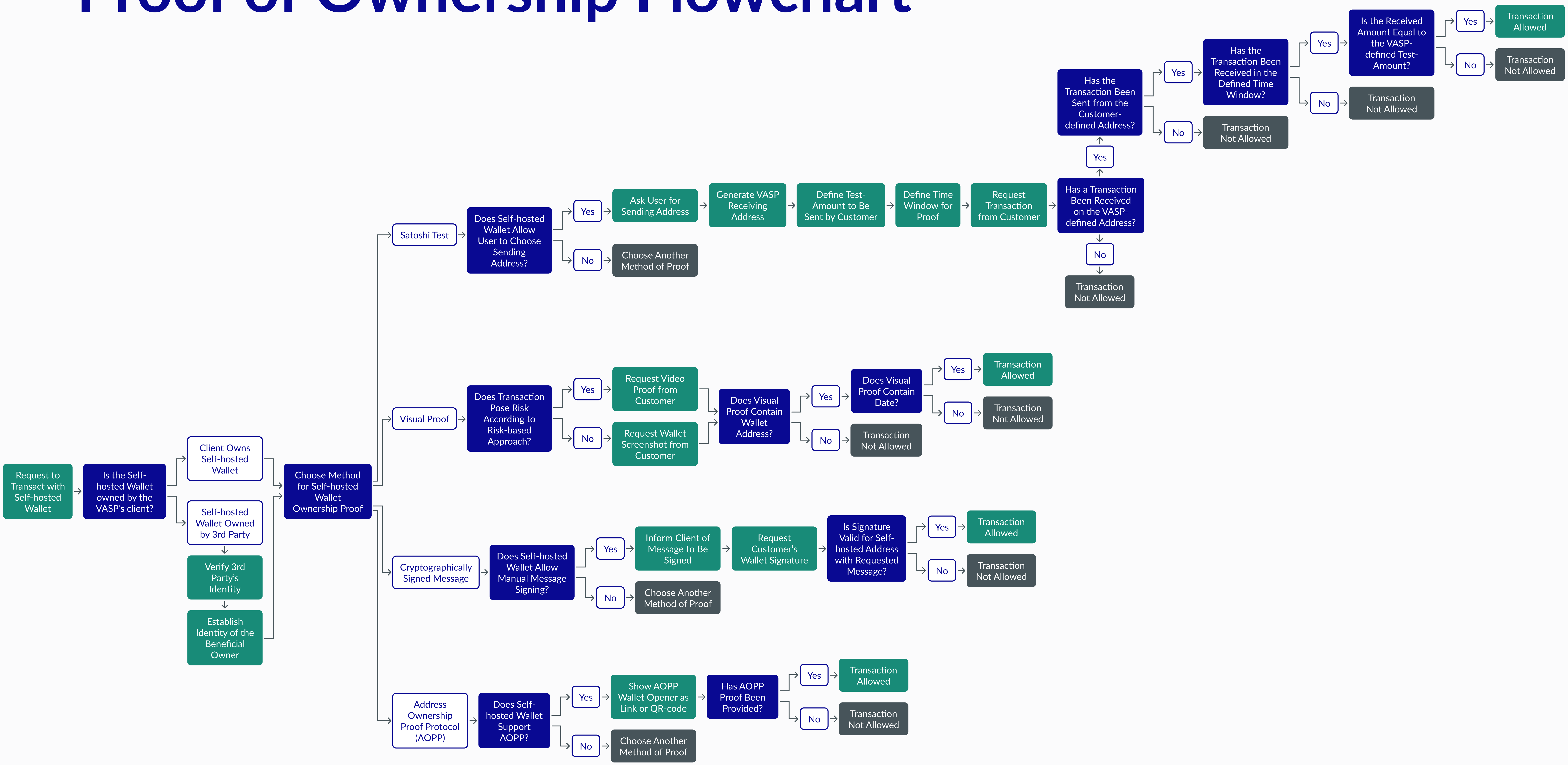
In short, this method automates the manual signing. Instead of having the customer connect to their self-hosted wallet, finding the signature feature, copying and pasting the defined message, and finally pasting the signature back to the VASP; with AOPP, most of these steps are automatically performed.

When requesting a transaction, AOPP allows customers to open their wallet software, which will automatically be pre-populated with the appropriate message from their VASP, and sign it with one click. The signature is immediately shared with the VASP, and the address is whitelisted in seconds. No manual work is required, and the customer can continue with their transaction as usual.

Consider Alex, who initiates a transaction using his wallet. With AOPP, Alex effortlessly whitelists his address during the transaction process, eliminating delays or additional steps. With one click, Alex can provide a signature for the required message, swiftly confirming ownership to the VASP.



Proof of Ownership Flowchart



Request to Transact with Self-hosted Wallet

Is the Self-hosted Wallet owned by the VASP's client?

Client Owns Self-hosted Wallet

Self-hosted Wallet Owned by 3rd Party

Verify 3rd Party's Identity

Establish Identity of the Beneficial Owner

Choose Method for Self-hosted Wallet Ownership Proof

Satoshi Test

Does Self-hosted Wallet Allow User to Choose Sending Address?

Yes

Ask User for Sending Address

Generate VASP Receiving Address

Define Test-Amount to Be Sent by Customer

Define Time Window for Proof

Request Transaction from Customer

Has a Transaction Been Received on the VASP-defined Address?

Yes

Has the Transaction Been Sent from the Customer-defined Address?

Yes

Has the Transaction Been Received in the Defined Time Window?

Yes

Is the Received Amount Equal to the VASP-defined Test-Amount?

Yes

Transaction Allowed

No

Transaction Not Allowed

No

Transaction Not Allowed

No

Transaction Not Allowed

No

Transaction Not Allowed

No

Choose Another Method of Proof

Visual Proof

Does Transaction Pose Risk According to Risk-based Approach?

Yes

Request Video Proof from Customer

No

Request Wallet Screenshot from Customer

Does Visual Proof Contain Wallet Address?

Yes

Does Visual Proof Contain Date?

Yes

Transaction Allowed

No

Transaction Not Allowed

No

Transaction Not Allowed

Cryptographically Signed Message

Does Self-hosted Wallet Allow Manual Message Signing?

Yes

Inform Client of Message to Be Signed

Request Customer's Wallet Signature

Is Signature Valid for Self-hosted Address with Requested Message?

Yes

Transaction Allowed

No

Transaction Not Allowed

No

Choose Another Method of Proof

Address Ownership Proof Protocol (AOPP)

Does Self-hosted Wallet Support AOPP?

Yes

Show AOPP Wallet Opener as Link or QR-code

Has AOPP Proof Been Provided?

Yes

Transaction Allowed

No

Transaction Not Allowed

No

Choose Another Method of Proof

21 ANALYTICS

MME

About the Authors

21 ANALYTICS

21 Analytics is the leading provider of Travel Rule compliance software, enabling businesses to keep transacting virtual assets in and out. 21 Travel Rule facilitates communication with counterparties globally, including self-hosted wallets, through its multiprotocol and privacy-first approach.

21 Analytics has been a leading developer in the Travel Rule ecosystem since 2020. We co-developed TRP, the Travel Rule Protocol by OpenVASP, an open-source, royalty-free standard for VASP-to-VASP communication, and built AOPP, for straightforward wallet verification by VASPs.

21analytics.ch

Lucas Betschart
CEO
lucas@21analytics.ch

Hannah Zacharias
Marketing & Regulatory Engagement Lead
hannah@21analytics.ch

About the Authors

MME

MME offers comprehensive and interdisciplinary advice in the areas of legal, tax and compliance: In these three areas MME provides integrated and well-coordinated services – speedy, efficient and always at the cutting edge. MME is one of the fastest growing and innovative advisory firms in the Greater Zurich Area; it supports and represents companies, families and private individuals in all economic and trendsetting matters. MME serves its clients with thorough, customer-centered attention: straightforward and persistent - in Switzerland and internationally.

mme.ch

Michèle Landtwing Leupi
Legal Partner
michele.landtwing@mme.ch

Fernando Tafur
Senior Legal Associate
fernando.tafur@mme.ch