Self-hosted Wallet Verification Made Easy

Address Ownership Proof Protocol

September 2024

Written by 21 Analytics

21 Travel Rule is the Only Solution for Transfers to Self-hosted Wallets

As part of Travel Rule compliance, some countries require originator and beneficiary identification when transactions involve a regulated entity and a self-hosted wallet.

To comply, VASPs must request, and store, a proof of ownership for the self-hosted wallet, according to the local regulations.

21 Travel Rule enables VASPs to easily request this proof without interrupting the customer journey via AOPP.

AOPP allows wallet owners to prove ownership with 1 click, and continue transacting seamlessly.

At the same time VASPs can enjoy the automated aspect of this verification method as no manual work is required, while ensuring compliance with the Travel Rule.

01 What Is AOPP?

AOPP (Address Ownership Proof Protocol) is an open standard used for proving self-hosted wallet ownership.

AOPP provides the same level of reliability as manual signing, 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.

"AOPP could solve the cumbersome proof of ownership issue." **[Cointelegraph]**

Delphine Forma, Policy Lead at Solidus Labs, and Crypto Compliance and Legal TG Founder.

02 Why VASPs Need AOPP

The European Union

The Transfer of Funds Regulation is the EU's implementation of the Travel Rule.
Crypto asset transfers in Europe must include information on the originator and beneficiary.
This information must be obtained, held, and shared with the crypto asset transfer counterparty and made available to competent authorities upon request.

Transfers involving CASPs and non-obliged entities (like self-hosted wallets) are also covered by the Regulation, which has specific requirements.

For transfers between CASPs and self-hosted wallets, CASPs must ensure the transfer can be individually identified.
This means CASPs need to collect the required Travel Rule information (name, physical address, and official personal document number).

Although these data points might already have been collected when the customer is onboarded, CASPs must guarantee that each transfer's originator and beneficiary can be individually identified.

Section 1, Article 14, Paragraph 5 of the TFR states:
"*In the case of a transfer of crypto-assets made to a self-hosted address, the crypto-asset service provider of the originator shall obtain and hold the information referred to in paragraphs 1 and 2 and shall ensure that the transfer of crypto-assets can be individually identified.*"

In transfers over EUR 1000, CASPs should verify whether the self-hosted address is effectively owned (or controlled) by their client.

03 Why VASPs Need AOPP

Switzerland

In August 2019, FINMA, the Swiss authority responsible for financial regulation, was one of the first regulators to issue its guidance on the application of the Travel Rule to VASPs, with a strict interpretation of the FATF's recommendations.

FINMA Guidance 02/2019 states the following for payments on the blockchain:

"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."

"If the customer is conducting an exchange (fiat-to-virtual currency, virtual-to-fiat currency, or virtual-to-virtual currency) and an external wallet is involved in the transaction, the customer's ownership of the self-hosted wallet must also be proven using suitable technical means."

This regulation means that any transaction involving a Swiss-regulated entity (e.g. VASP or a bank) and a non-regulated entity (e.g. a self-hosted wallet) will demand at least an ownership proof of the wallet.

VASPs that fall directly under FINMA's supervision - such as banks - and members of a self-regulatory organisation (SRO) have to follow the regulation. This is especially relevant considering that most Swiss VASPs are members of an SRO, particularly the Financial Services Standards Association (VQF).

Per the VQF (Article 14, Paragraph 1) Regulations:

"Payment transactions to and from external wallets are only permitted where the wallets are owned by a member's own customer. The customer's authority over the external wallet must be verified using suitable technical measures. Transactions between customers of the same member are permitted."

04 Why VASPs Need AOPP

United Kingdom

In the UK, Cryptoasset businesses are to first apply a risk-based approach and assess the risks the wallet address could pose according to the Money Laundering, Terrorist Financing and Proliferate Financing standards, then request the Travel Rule data.

If the transfer is deemed high-risk, self-wallet verification is required, with the FCA specifically citing micro-deposits (Satoshi Tests) and cryptographic signatures, like AOPP.

Moreover, additional originator Travel Rule data may be requested with transactions over EUR 1000 based on a risk analysis. This data can include the customer identification number, address, birth certificate number, passport number, national identity card number, or date and place of birth.

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

Germany

Transactions with self-hosted wallets fall under Germany's implementation of the Travel Rule if an obliged entity is involved in the transfer of virtual assets. Therefore, peer-to-peer transfers are excluded.

Obliged entities must assess and determine the transfer's AML/CFT risks using risk-appropriate measures that ensure traceability. Per **Section 4 KryptoWTransferV**, collecting, storing, and checking the wallet's owner's name and address is risk-appropriate. Therefore, proof of ownership must be carried out.

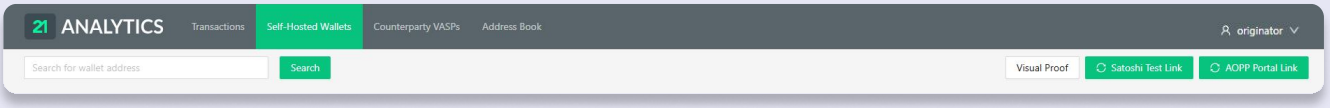
However, this is set to change by 30 December 2024 when Germany becomes aligned with the European Union's Travel Rule (Transfer of Funds Regulation).

05

21 Travel Rule & AOPP

From the VASP's Perspective

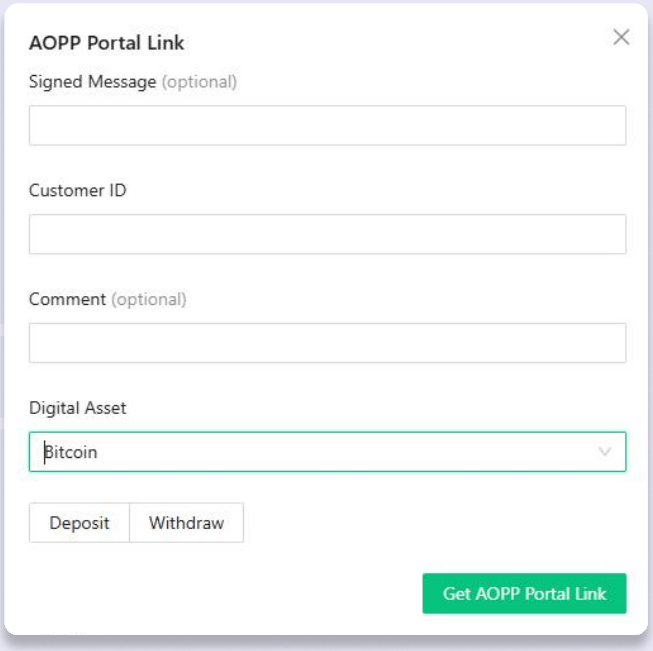
To get started, the VASP will need to click on the **Self-hosted Wallets** tab. Once the tab is opened, wallet verification methods will be displayed in the top right hand side corner click. **AOPP Portal Link** is to be selected.



Next a pop-up will open requesting the following information:

- the Customer ID (provided from your customer database, e.g. core banking system),
- the digital asset address type,
  if selecting bitcoin, the transaction type - Deposit or Withdraw - is to be confirmed.

The VASP will complete this information and click **Get AOPP Portal Link**

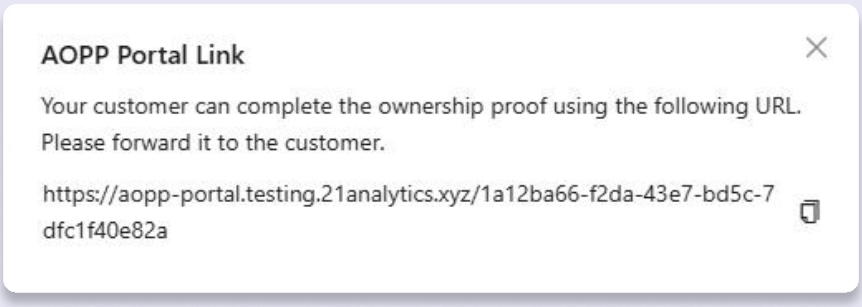


06 21 Travel Rule & AOPP

From the VASP's Perspective

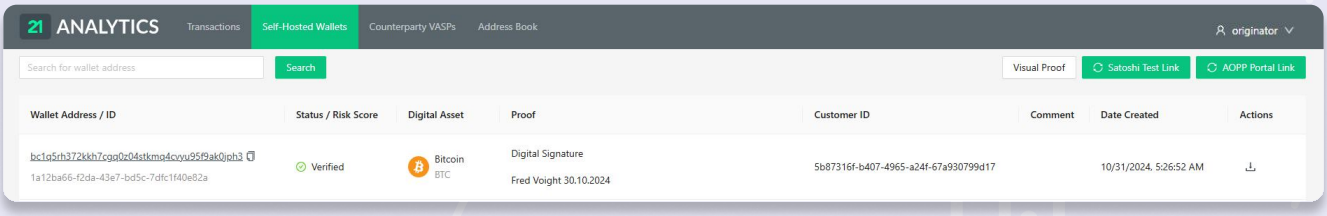
An **AOPP Portal Link** will be generated which the VASP can now share with their customer via their choice of communication channel.

Once used to successfully validate an address ownership proof, the link cannot be reused.



Opening the link in their browser, the customer will complete the required steps.

After the wallet owner has submitted the ownership proof, it will appear automatically under **Self-hosted Wallets** tab in the **21 Travel Rule Compliance Dashboard**, along with its risk score.



As the customer was previously KYC'd, no further compliance-related action will be required from the VASP.

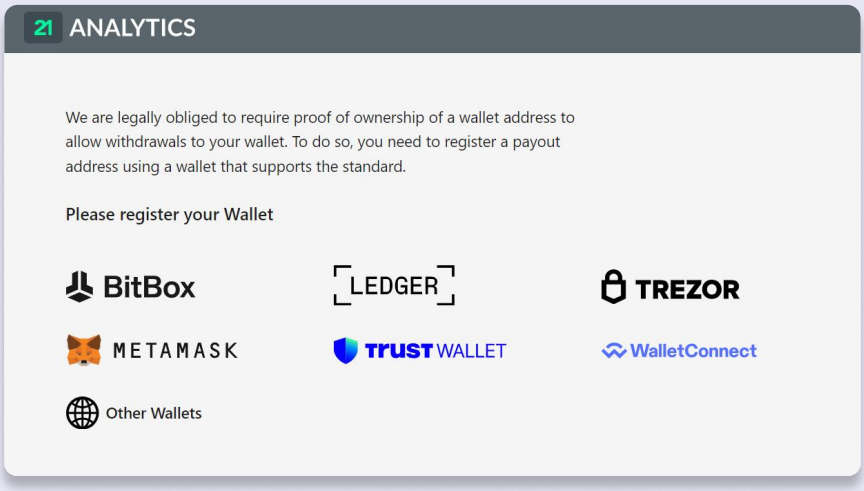
07

21 Travel Rule & AOPP

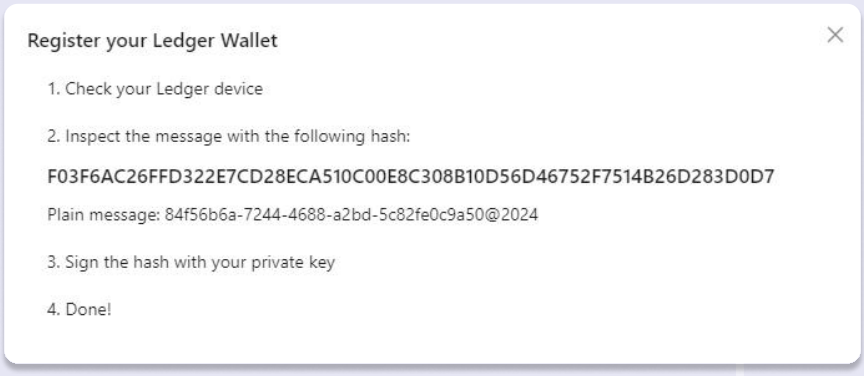
From the Wallet Owner's Perspective

The VASP will send the wallet owner a link via their preselected communication channel.

The wallet owner will open the **AOPP Portal Link**. Once opened they will need to select their wallet type in the **AOPP Portal.**



After selecting their wallet type, a pop-up will appear directing them to their device with further instructions on how to complete the ownership proof.



08

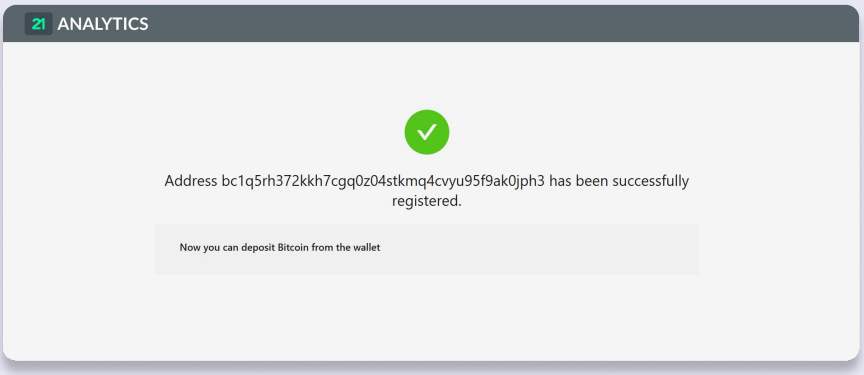
21 Travel Rule & AOPP

From the Wallet Owner's Perspective

Once the wallet owner has completed the ownership proof process following the prompts per their wallet, the will receive 2 confirmation messages.

One message will appear on their wallet confirming their address is now ready for transacting.
(Please note, the exact wording of this message does vary between wallets.)

The second message will automatically appear in the **AOPP Portal**, confirming their address has been successfully registered and that they are able to transact.



09 AOPP Success Story: Relai

Relai Leverages 21 Analytics to Sell Bitcoin Compliantly

Relai had the goal of becoming a one-stop shop for easy bitcoin investment.
To fulfil this goal, Relai's founders decided to incorporate brokerage functions into their business. However, this decision brought challenges to their operations, especially to the compliance team.

Relai had always offered self-hosted wallet services. But now, being registered as a VASP and allowing their customers to buy bitcoin to their Relai wallet or any other self-hosted wallet, they needed to comply with FINMA's requirements.

To meet FINMA's requirements and provide as little friction as possible to their users' experience, Relai turned to 21 Travel Rule, specifically AOPP.

As ownership proofs are fully automated with AOPP, compliance is easy for customers and Relai, alike. In fact, AOPP offered Relai 2 giant advantages: an excellent user experience and easy software integration.

According to Relai, the great user experience allowed **each and every** transaction to go through automatically, keeping users engaged without adding difficulties or breaks in their journeys.

Moreover, its implementation was a breeze: summing up all integration efforts necessary, the CTO did not dedicate more than two (2!) hours.

"We want to empower the customer to do everything on mobile, so connecting hardware wallets to Android smartphones for easier proofs is key: and 21 Analytics' solution is what enables this amazing compliance experience."

Adem Bilicen, CTO, Relai.

10 What Next?

How 21 Analytics Can Support Your Team

Do you have questions that weren't tackled in this explainer?

Perhaps you are unsure of how AOPP can fit into your current solution or compliance strategy.

Reach out to one of our experts.

Request a Demo

AOPP's Advantages

AOPP does not require address reuse and so preserves conventional best practices for your business' confidentiality.
Best of all it is Travel Rule, FINMA, and GDPR compliant.

It reduces the risks of MITM attacks from crypto-malware as addresses are not copied and pasted as in traditional manual signing methods.

AOPP is more reliable than screenshots and video proofs, which can be manipulated easily by senders.
Moreover, it is easier and cheaper to perform when compared to Satoshi Tests.

21 Analytics AG Zug, Switzerland

info@21analytics.ch
www.21analytics.ch

21analytics.ch/what-is-aopp