Unhosted wallets

Dr Alexander Ressos, TEP
Of Counsel, KGP Legal LLC
Attorney-at-Law (Switzerland and Germany), Solicitor (England & Wales and Hong Kong)

The hardest case is the transfer to or from a wallet whose keys are held by a private person without any institution behind it. The FATF calls these "unhosted" or "self-hosted" wallets. There is no beneficiary institution to receive the information or to verify the beneficiary, so the rule as drafted cannot apply in full. MAS's position, set out in the Guidelines, is that the licensee must still obtain the required originator and beneficiary information from its own customer and record it. The licensee must apply risk-based measures to assess whether the unhosted wallet belongs to the customer or to a third party. Transfers to third-party unhosted wallets are treated as higher-risk for monitoring purposes.[1] MAS has stopped short of requiring proof of ownership for every unhosted-wallet transfer.

Switzerland went further. FINMA's Guidance 02/2019 of 26 August 2019 requires a Swiss financial intermediary that transfers crypto assets to or from an external wallet to verify by suitable technical means that the wallet belongs to its own customer. Otherwise the counterparty is a third party whose identity must be established as in a wire transfer, which in practice means the transfer cannot be made.[2] The Swiss position closed off anonymous withdrawals to third parties. The Singapore position permits them under a risk-based regime. A group operating in both hubs must therefore choose. It can run the stricter Swiss standard globally, which is simpler and defensible in Singapore as exceeding the requirement. Or it can run two standards, which is cheaper for the Singapore customer base and more complex to govern. Chapter VIII returns to the choice.

Proving control of a wallet

Whichever standard a firm adopts, it needs a method for verifying that a customer controls an external address. Three methods are in use. The signed-message method asks the customer to sign a message containing a nonce with the private key of the address, which the firm verifies against the public key. The micro-transfer method asks the customer to send a specified small amount from the address within a window. The screenshot method asks for a screenshot of the wallet software showing the address, which proves nothing and should not be used.[3] The signed-message method is the most reliable and the only one that works without moving value. Firms should record the signed message and the verification result in the customer file and should re-verify when a customer declares a new address.

Example

A Singapore MPI's corporate customer, a Zug GmbH that develops a decentralised exchange, instructs the withdrawal of 1,000,000 USDC to an address it describes as the protocol's treasury multisig. The

Copyright © 2026 Dr Alexander Ressos, TEP – Of Counsel, KGP Legal LLC. SingaporeIQ is an information website and gives no legal advice. For Singapore law advice through KGP Legal LLC, please write to alexander.ressos@kgplegal.com.sg

address is a smart-contract wallet controlled by five signers of whom three must agree. No single private key corresponds to it, so the signed-message method fails in its simple form. The MPI has three options. It can ask the signers to execute an on-chain message from the multisig, since most multisig implementations support signing through a standard interface. It can request a micro-transfer from the multisig. Or it can document the multisig's ownership through the protocol's public governance records and the GmbH's board resolution identifying the signers. The MPI chooses the first, records the verification, rates the destination as "customer-controlled, higher complexity", and sets a monitoring rule that flags any later transfer from the treasury to an address not previously seen.

Notes

1. Guidelines to Notice PSN02, section on value transfers involving unhosted wallets, requiring the licensee to collect and record originator and beneficiary information from its customer and to apply risk-based measures including, where appropriate, verification of the customer's control over the wallet.
2. FINMA Guidance 02/2019, Payments on the blockchain, 26 August 2019, on the application of Art. 10 AMLO-FINMA to transfers to and from external wallets; see Part F, Chapter IV.
3. Guidelines to Notice PSN02, section on unhosted wallets, referring to the use of technical means such as cryptographic signing to verify ownership; FINMA Guidance 02/2019 uses the same concept ("geeignete technische Mittel").

Copyright © 2026 Dr Alexander Ressos, TEP – Of Counsel, KGP Legal LLC. SingaporeIQ is an information website and gives no legal advice. For Singapore law advice through KGP Legal LLC, please write to alexander.ressos@kgplegal.com.sg