Multi-party computation and multi-signature

Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland and Germany),
Solicitor (England & Wales and Hong Kong)
Of Counsel, KGP Legal LLC
alexander.ressos@kgplegal.com.sg
www.ressos.com.sg

Two technologies have replaced the single private key in institutional custody. Multi-signature (multisig) is a feature of the ledger itself. An address is configured so that, say, two of three keys must sign any transaction. Multi-party computation (MPC) achieves a similar result off-chain. The private key is never assembled. Instead several parties hold shares of it and jointly compute a signature without any party learning the whole key. Fireblocks, Copper and most bank-grade custody platforms use MPC.

The legal significance is that "who holds the key" no longer has a single answer. If a client holds one share and the custodian holds two in a two-of-three scheme, the custodian can move the assets alone. If the client holds two shares, the custodian cannot. If each of client, custodian and a third-party recovery provider holds one share, no single party has control. Each configuration produces a different answer to the questions whether the custodian has "possession or control" for Singapore licensing purposes, whether the custodian "holds" the assets for Swiss segregation purposes, and who has the factual power of disposal that Swiss private law treats as the connecting factor.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Practice note

When you review a custody arrangement built on MPC or multisig, obtain a diagram of key shares and signing thresholds and ask, for each possible combination of parties, whether that combination can move the assets. Then ask who can change the configuration. An MPC platform that lets the custodian re-share keys unilaterally gives the custodian control, whatever the headline threshold says. Record the answer in the opinion. A Singapore licensing analysis or a Swiss segregation opinion that does not state the key-share configuration is incomplete.

FINMA has treated the holding of one key share as sufficient to bring a provider within the AMLA perimeter if that share lets the provider initiate or block transfers.[1] MAS has not published a formal position on key shares but has applied the "possession or control" test in licensing decisions in a way that catches providers who can transfer customer assets without customer action.

Notes

1. FINMA Guidance 02/2019 of 26 August 2019, section 3; FINMA, Annual Report 2020, section on fintech supervision (power of disposal through partial keys). Part F, Chapter II. ↩

Disclaimer

This article is provided for general information only. It is based on publicly available sources as at its date of publication. These sources have not been independently verified against licences, regulatory registers or the records of the entities concerned. It is not legal, tax, financial or investment advice. Nor is it a recommendation to invest in, transact with or use the services of any entity mentioned. Law and regulation change frequently, so the content may be incomplete or outdated. To the fullest extent permitted by law, Dr Alexander Ressos and the publisher of SingaporeIQ exclude all liability for loss or damage arising from the use of or reliance on this article. Readers should obtain advice on their specific circumstances before acting or refraining from action.

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.

Names and trademarks of the entities discussed belong to their owners and are used for identification only. Their mention implies no endorsement, affiliation or allegation of wrongdoing. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. Corrections and updates: contact@ressos.com.

© 2026 Dr Alexander Ressos. This article may be quoted with attribution to SingaporeIQ (SingaporeIQ.com). Reproduction in full and any commercial use require prior written consent. The Legal Terms at https://singaporeiq.com/legal-terms apply.

Author contact: Dr Alexander Ressos, TEP · contact@ressos.com

© 2026 Dr Alexander Ressos. General information only, not legal, tax or investment advice. No client relationship is created. All Singapore law advice is provided by a duly licensed and regulated firm of Singapore advocates and solicitors only on the basis of an express written letter of engagement. More information at SingaporeIQ.com and ressos.com.sg.