Multi-Party Computation und Multi-Signatur

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

Zwei Technologien haben den einzelnen privaten Schlüssel in der institutionellen Verwahrung abgelöst. Multi-Signatur (Multisig) ist eine Funktion des Registers selbst. Eine Adresse wird so konfiguriert, dass beispielsweise zwei von drei Schlüsseln jede Transaktion signieren müssen. Multi-Party Computation (MPC) erreicht ein ähnliches Ergebnis außerhalb der Chain. Der private Schlüssel wird nie zusammengesetzt. Stattdessen halten mehrere Parteien Anteile daran und berechnen gemeinsam eine Signatur, ohne dass eine Partei den ganzen Schlüssel erfährt. Fireblocks, Copper und die meisten Verwahrplattformen auf Bankniveau verwenden MPC.

Rechtlich bedeutsam ist, dass die Frage „Wer hält den Schlüssel?“ keine einzige Antwort mehr hat. Hält in einem Zwei-von-drei-Schema der Kunde einen Anteil und der Verwahrer zwei, kann der Verwahrer die Vermögenswerte allein bewegen. Hält der Kunde zwei Anteile, kann der Verwahrer es nicht. Halten Kunde, Verwahrer und ein dritter Wiederherstellungsdienst je einen Anteil, hat keine einzelne Partei die Kontrolle. Jede Konfiguration beantwortet anders, ob der Verwahrer für das Singapurer Lizenzrecht „possession or control“ hat, ob er die

© 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.

Vermögenswerte für die Schweizer Aussonderung „hält“ und wer die tatsächliche Verfügungsmacht innehat, die das Schweizer Privatrecht als Anknüpfungspunkt behandelt.

Praxishinweis

Wenn Sie eine Verwahrungsgestaltung auf Basis von MPC oder Multisig prüfen, lassen Sie sich ein Diagramm der Schlüsselanteile und Signaturschwellen geben. Fragen Sie dann für jede mögliche Kombination von Parteien, ob diese Kombination die Vermögenswerte bewegen kann. Fragen Sie anschließend, wer die Konfiguration ändern kann. Eine MPC-Plattform, die dem Verwahrer erlaubt, Schlüssel einseitig neu aufzuteilen, verschafft ihm die Kontrolle, gleichgültig, was die angegebene Schwelle besagt. Halten Sie die Antwort im Gutachten fest. Eine Singapurer Lizenzanalyse oder ein Schweizer Aussonderungsgutachten, das die Konfiguration der Schlüsselanteile nicht nennt, ist unvollständig.

Die FINMA hat das Halten eines einzigen Schlüsselanteils als ausreichend angesehen, um einen Anbieter dem Geldwäschereigesetz zu unterstellen, wenn dieser Anteil es ihm erlaubt, Übertragungen auszulösen oder zu blockieren.[1] Die MAS hat keine förmliche Position zu Schlüsselanteilen veröffentlicht. Sie hat den Test „possession or control“ in Lizenzentscheidungen aber so angewandt, dass Anbieter erfasst werden, die Kundenvermögen ohne Zutun des Kunden übertragen können.

Anmerkungen

1. FINMA-Aufsichtsmitteilung 02/2019 vom 26. August 2019, Abschnitt 3; FINMA, Jahresbericht 2020, Abschnitt zur Fintech-Aufsicht (Verfügungsmacht über Teilschlüssel). Teil F, Kapitel II. ↩

© 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.

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.

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