Computación multipartita y firma múltiple

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

Dos tecnologías han sustituido a la clave privada única en la custodia institucional. La firma múltiple (multisig) es una función del propio registro. Una dirección se configura de modo que, por ejemplo, dos de tres claves deban firmar cualquier transacción. La computación multipartita (MPC, multi-party computation) logra un resultado similar fuera de la cadena. La clave privada nunca llega a ensamblarse. En su lugar, varias partes poseen fragmentos de ella y calculan conjuntamente una firma sin que ninguna llegue a conocer la clave completa. Fireblocks, Copper y la mayoría de las plataformas de custodia de nivel bancario utilizan MPC.

La relevancia jurídica es que la pregunta «quién posee la clave» ya no tiene una única respuesta. Si en un esquema de dos de tres el cliente posee un fragmento y el custodio dos, el custodio puede mover los activos por sí solo. Si el cliente posee dos fragmentos, el custodio no puede. Si el cliente, el custodio y un proveedor externo de recuperación poseen un fragmento cada uno, ninguna parte tiene el control por sí sola. Cada configuración da una respuesta distinta a las preguntas de si el custodio tiene «la posesión o el control» a efectos de las licencias de Singapur, si el custodio «mantiene» los activos a efectos de la segregación suiza y quién tiene el poder de disposición fáctico que el Derecho privado suizo trata como criterio de conexión.

© 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.

Nota práctica

Cuando revise un esquema de custodia basado en MPC o en firma múltiple, obtenga un diagrama de los fragmentos de clave y de los umbrales de firma y pregúntese, para cada combinación posible de partes, si esa combinación puede mover los activos. Después, pregunte quién puede modificar la configuración. Una plataforma MPC que permite al custodio redistribuir los fragmentos de clave unilateralmente le otorga el control, diga lo que diga el umbral nominal. Deje constancia de la respuesta en el dictamen. Un análisis de licencias en Singapur o un dictamen sobre segregación en Suiza que no indique la configuración de los fragmentos de clave está incompleto.

FINMA ha considerado que la tenencia de un solo fragmento de clave basta para que un proveedor quede dentro del perímetro de la Ley suiza contra el blanqueo de capitales (GwG/LBA) si ese fragmento le permite iniciar o bloquear transferencias.[1] La Monetary Authority of Singapore (MAS, la autoridad monetaria y supervisora financiera) no ha publicado una posición formal sobre los fragmentos de clave, pero ha aplicado la prueba de «posesión o control» en sus decisiones sobre licencias de un modo que alcanza a los proveedores capaces de transferir activos de los clientes sin intervención de estos.

Notas

1. Comunicación FINMA 02/2019, de 26 de agosto de 2019, sección 3; FINMA, Informe anual 2020, apartado sobre la supervisión fintech (poder de disposición mediante claves parciales). Parte F, capítulo 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

© 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.

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

© 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.