Calcul multipartite et multisignature

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

Deux technologies ont remplacé la clé privée unique dans la conservation institutionnelle. La multisignature (multisig) est une fonctionnalité du registre lui-même. Une adresse est configurée de telle sorte que, par exemple, deux clés sur trois doivent signer toute transaction. Le calcul multipartite (multi-party computation, MPC) aboutit à un résultat similaire hors chaîne. La clé privée n'est jamais assemblée. Plusieurs parties en détiennent chacune une part et calculent conjointement une signature sans qu'aucune d'elles ne prenne connaissance de la clé entière. Fireblocks, Copper et la plupart des plateformes de conservation de niveau bancaire utilisent le MPC.

La portée juridique est que la question « qui détient la clé » n'a plus de réponse unique. Si, dans un schéma deux sur trois, le client détient une part et le dépositaire deux, le dépositaire peut déplacer les actifs seul. Si le client détient deux parts, le dépositaire ne le peut pas. Si le client, le dépositaire et un prestataire tiers de récupération détiennent chacun une part, aucune partie n'a seule le contrôle. Chaque configuration appelle une réponse différente à trois questions : le dépositaire a-t-il la « possession ou le contrôle » au sens du régime d'autorisation singapourien,

© 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.

« détient »-il les actifs au sens des règles suisses de ségrégation, et qui dispose du pouvoir de disposition de fait que le droit privé suisse retient comme critère de rattachement ?

Note pratique

Lorsque vous examinez un dispositif de conservation fondé sur le MPC ou la multisignature, procurez-vous un schéma des parts de clés et des seuils de signature. Demandez, pour chaque combinaison possible de parties, si cette combinaison peut déplacer les actifs. Demandez ensuite qui peut modifier la configuration. Une plateforme MPC qui permet au dépositaire de redistribuer unilatéralement les parts de clés lui confère le contrôle, quel que soit le seuil affiché. Consignez la réponse dans l'avis. Une analyse au regard du régime d'autorisation singapourien ou un avis suisse sur la ségrégation qui n'indique pas la configuration des parts de clés est incomplet.

La FINMA a considéré que la détention d'une seule part de clé suffit à faire entrer un prestataire dans le périmètre de la LBA si cette part lui permet d'initier ou de bloquer des transferts.[1] La MAS n'a pas publié de position formelle sur les parts de clés, mais elle a appliqué le critère de la « possession ou du contrôle » dans ses décisions d'autorisation d'une manière qui englobe les prestataires capables de transférer les actifs des clients sans intervention de ces derniers.

Notes

1. Communication FINMA 02/2019 du 26 août 2019, section 3 ; FINMA, rapport annuel 2020, section sur la surveillance des fintechs (pouvoir de disposition au moyen de clés partielles). Partie F, chapitre 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