다자간 연산과 다중서명

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

기관 보관에서는 두 가지 기술이 단일 개인 키를 대체했습니다. 다중서명(multi-signature, multisig)은 원장 자체의 기능입니다. 예를 들어 어떤 거래든 키 세 개 중 두 개가 서명해야 하도록 주소를 설정합니다. 다자간 연산(multi-party computation, MPC)은 비슷한 결과를 체인 밖에서 달성합니다. 개인 키는 한 번도 조립되지 않습니다. 대신 여러 당사자가 키의 조각을 나누어 보유하고, 어느 당사자도 전체 키를 알지 못한 채 공동으로 서명을 계산합니다. Fireblocks, Copper를 비롯한 대부분의 은행급 보관 플랫폼이 MPC를 사용합니다.

법적 의미는 '누가 키를 보유하는가'에 더 이상 하나의 답이 없다는 점입니다. 3개 중 2개 방식에서 고객이 조각 하나를, 수탁업자가 조각 둘을 보유하면 수탁업자는 단독으로 자산을 옮길 수 있습니다. 고객이 조각 둘을 보유하면 수탁업자는 옮길 수 없습니다. 고객, 수탁업자, 제3의 복구 서비스 제공자가 각각 조각 하나씩 보유하면 어느 한 당사자도 통제권을 갖지 않습니다. 구성마다 다음 질문들에 대한 답이 달라집니다. 싱가포르 라이선스 목적상 수탁업자가 '점유 또는 통제권'을 갖는가, 스위스 분리 보관 목적상 수탁업자가 자산을 '보유'하는가, 그리고 스위스 사법이 연결점으로 삼는 사실상의 처분권은 누구에게 있는가입니다.

© 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.

실무 메모

MPC나 다중서명에 기반한 보관 약정을 검토할 때에는 키 조각과 서명 기준을 보여 주는 도식을 확보하고, 가능한 모든 당사자 조합에 대해 그 조합이 자산을 옮길 수 있는지 물어보십시오. 그다음 누가 구성을 바꿀 수 있는지 물어보십시오. 수탁업자가 일방적으로 키를 재분배할 수 있게 하는 MPC 플랫폼은 표면상의 서명 기준이 무엇이든 수탁업자에게 통제권을 줍니다. 그 답을 의견서에 기록하십시오. 키 조각 구성을 명시하지 않은 싱가포르 라이선스 분석이나 스위스 분리 보관 의견서는 불완전합니다.

FINMA는 키 조각 하나를 보유하더라도 그 조각으로 이전을 개시하거나 차단할 수 있다면 제공자를 자금세탁방지법(AMLA)의 규제 범위에 포함시키기에 충분하다고 보아 왔습니다.[1] MAS는 키 조각에 관한 공식 입장을 발표하지 않았습니다. 다만 라이선스 결정에서 '점유 또는 통제' 기준을 적용하면서, 고객의 행위 없이 고객 자산을 이전할 수 있는 제공자를 규제 대상에 포함시켜 왔습니다.

주

1. FINMA Guidance 02/2019, 2019년 8월 26일, section 3; FINMA, Annual Report 2020, 핀테크 감독에 관한 부분(부분 키를 통한 처분권). 제F편 제II장. ↩

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 Law and regulation change frequently, so the content may be incomplete or outdated.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.