(翻译本)

本局档号：B1/15C
G16/1C

致：所有认可机构
行政总裁

敬启者：

提供数码资产保管服务

随着数码资产产业持续发展，香港金融管理局(金管局)留意到认可机构对数码资产[1]相关活动，尤其为客户提供数码资产保管服务的兴趣日益浓厚。

为确保认可机构保管的客户数码资产得到充分保障，同时相关风险得到妥善管理，金管局认为有需要就认可机构提供数码资产保管服务提供指引。金管局参考国际标准及做法，制定附件所载的预期标准，并赋予认可机构灵活性，可因应所保管的数码资产的性质、特点及风险制定相称的运作安排。认可机构应按照该等标准保障客户数码资产，不论认可机构是在以中介人身分进行虚拟资产相关活动[2]、在分销代币化产品或是在提供独立的保管服务的过程中收取该等资产。

除附件所载的预期标准外，认可机构在提供数码资产保管服务时亦应遵守所有适用法律及监管规定。

本通告适用于进行数码资产保管活动的认可机构及本地注册认可机构的附属公司。本地注册认可机构应确保该等附属公司的业务操守、作业方式 及监控措施均符合本通告及附件。

[1] 就本通告而言，「数码资产」一词指主要依赖加密及分布式分类账或类似技术的数码资产，例如《打击洗钱及恐怖分子资金筹集条例》(《打击洗钱条例》)第53ZRA条所界定的虚拟资产、代币化证券及其他代币化资产。此外，「数码资产」一词应理解为亦涵盖接达数码资产的方式，一般是指私人密钥、种子或其备份。《打击洗钱条例》第53ZR条所界定的有限用途数码代币则不在本通告的涵盖范围内。本通告不适用于认可机构或其集团公司保管并非代表客户持有的自营资产。

[2] 见金管局与证券及期货事务监察委员会发出的「有关中介人的虚拟资产相关活动的联合通函」(最新于 2023 年 12 月 22 日更新)。

实施

如认可机构或(如属本地注册认可机构)其附属公司有意提供数码资产保管服务，应事先与金管局商讨，并向金管局显示并使其信纳它们符合本通告所载的预期标准及规定(及经不时修订的该等标准及规定)。

如认可机构或本地注册认可机构的附属公司已开展数码资产保管活动，应审视及按需要修订其系统与监控措施。该等认可机构或其附属公司已开展数码资产保管活动的本地注册认可机构应在本通告日期起计 **6** 个月内通知金管局及确认其已符合附件所载的预期标准。

金管局会密切留意迅速发展的数码资产市场及国际监管环境，如有需要，可提供进一步指引。贵机构如对本通告有任何问题，请联络周佑旌先生(2878-8310)或陈嘉霖女士(2878-1210)。

助理总裁(银行操守)
区毓麟

2024 年 2 月 20 日

连附件

副本送：证券及期货事务监察委员会 (收件人：中介机构部临时主管蔡钟辉先生)

附件

有关认可机构提供数码资产保管服务的预期标准的指引

本指引适用于认可机构及本地注册认可机构的附属公司[3]代客户持有的数码资产(即主要依赖加密及分布式分类账或类似技术的数码资产)(下文称为「客户数码资产」)的保管活动，但不包括有限用途数码代币[4]。所涵盖资产包括虚拟资产[5]、代币化证券及其他代币化资产[6]。本指引不适用于认可机构或其集团公司保管并非代表客户持有的自营资产。

(A) 管治及风险管理

1. 认可机构在推出数码资产保管服务前，应进行全面的风险评估，以识别及了解相关风险。认可机构应在考虑适用的法律及监管规定后，制定适当的政策、程序及监控措施，以管理及缓解所识别的风险。认可机构的董事局及高级管理层应对风险管理过程实施有效监察，以确保在从事保管活动前及持续地识别、评估、管理及缓解与保管活动相关的风险。

2. 认可机构应就其保管活动分配充足资源，包括所需人手及专业知识， 以确保妥善的管治、运作及有效的风险管理。高级管理层及负责进行认可机构的保管活动与相关监控职能的职员应具备所需知识、技能及专业知识，以履行其职责。

3. 鉴于数码资产市场发展迅速，认可机构应确保向高级管理层及参与保管活动的职员提供充足培训，使其能持续具备胜任能力。

4. 认可机构应就保管活动设有适当的问责安排，包括以书面形式清楚列明角色与责任，以及汇报途径。认可机构亦应设有充足的政策及程序，

---

[3] 就本附录其余部分而言，「认可机构」一词包括本地注册认可机构的附属公司提供数码资产保管服务。

[4] 如《打击洗钱条例》第 53ZR 条所界定。

[5] 如《打击洗钱条例》第 53ZRA 条所界定。

[6] 「代币化证券」及「其他代币化资产」一般指以分布式分类账或类似技术记录拥有权的数码形式证券(「证券」定义如《证券及期货条例》所界定)及数码形式的其他现实世界资产。

以识别、管理及缓解可能产生的任何潜在及／或实际利益冲突，例如在认可机构或其附属成员进行的不同活动之间所产生的任何潜在及／或实际利益冲突。

5. 认可机构应制定及维持有效的应变及灾难复原安排，以确保其保管活动可持续运作。

(B) 分隔客户数码资产

6. 认可机构应在独立的客户账户[7]持有客户数码资产，与认可机构本身的资产分隔，以确保一旦认可机构无力偿债或进入处置程序时，能保护客户数码资产免受认可机构债权人的申索影响。

7. 认可机构不应转移客户数码资产的任何权利、拥有权、法定及／或实益所有权，或以其他方式借出、质押、再质押客户数码资产或对客户数码资产设定任何产权负担，惟以下情况除外：(i)交易的交收，及／或支付客户欠认可机构的费用及收费；(ii) 事前已取得客户的明确书面同意；或(iii)法律规定。认可机构应设有充足及有效措施，以防范认可机构为其本身账户或为与其客户商定以外的任何其他目的使用客户数码资产。

(C) 保障客户数码资产

8. 认可机构应设有充足的系统及监控措施，以确保客户数码资产尽快及妥善地加以记账及获得充分保障。尤其是，认可机构应设有有效监控措施，以减低因盗窃、欺诈、疏忽或其他挪用行为，以及延误接达或未能接达客户数码资产而导致客户数码资产有任何损失的风险。

9. 认可机构可采取风险为本方法，因应所保管的数码资产的性质、特点及风险，制定系统与监控措施以保障客户数码资产。举例来说，风险会视乎所用的分布式分类账技术(DLT)网络(例如私有许可制、公有许可制及公有非许可制)，以及所设立的缓解措施。例如与设有DLT 网

[7] 包括于分布式分类账持有客户数码资产的钱包地址，而有关钱包地址应与用作持有认可机构 本身资产的钱包地址分隔。

络接达权限制的公有许可制及私有许可制 DLT 网络相比，于公有非许可制DLT网络以非许可制代币形式持有客户数码资产，可能会面对更高的网络保安风险，亦可能于发生盗窃、黑客入侵或其他网络攻击后，难以追回所失去的资产。

10. 保障客户数码资产的系统与监控措施包括有关以下各方面的书面政策及程序等：

- 授权及核实以进行客户数码资产存入、提取及转移的接达，包括储存种子及私人密钥的装置的接达；及

- 管理及保障客户数码资产的种子及私人密钥，范围涵盖密钥的产生、分派、储存、使用、销毁及备份。

11. 尤其是，认可机构应采纳相关业内最佳作业手法，并遵循适用国际保安标准，以与所持有资产的性质、特点及风险相称的方式保障客户数码资产。尽管下述程序及监控措施不拟作为硬性规定或适用于所有情况，但若认可机构持有客户虚拟资产，一般都必须实施该等程序及监控措施。就其他数码资产而言，认可机构可采用风险为本方法，按与所造成的风险相称的方式实施下述程序及监控措施；惟如该数码资产属于公有非许可制DLT网络上的非许可制代币，认可机构应格外审慎，严谨地评估以下程序及监控措施的实施：

- 在安全及防窜改的环境及装置(例如以硬件安全模块(Hardware Security Module)，简称 HSM)中产生及储存种子及私人密钥，包括其备份。在实际可行情况下，应以脱机方式产生种子及私人密钥，并设有适当的生命周期上限；

- 在香港以安全的方式产生、储存及备份种子及私人密钥；

- 按有需要知道的基础，严格限制对加密装置或应用程序的存取，只限经适当甄选及培训的获授权人士进行；备存最新的文件，以记录 如何授权及核实接达权，以及如何分配接达权；使用可靠有力的认 证方法(如多重认证)确认对种子及私人密钥的接达权；备存有关接达加密装置或应用程序的审计线索；

- 实施稳健的监控措施，以避免出现任何缺失的可能，例如藉利用密钥分片或类似技术分拆及分散私人密钥，在认可机构授权的多名人员之间进行分散储存，从而并无单一人士可持有有关密钥的完整资料。在一般情况下，一定数目的密钥分片持有人须集体行事，共同签订一项交易，以确保并无单一人士可管有完整的接达权，并可同时防范因某一分片遗失、无法取得或被盗而令运作中断。为防范出现缺失的可能，亦可考虑使用多个钱包而非单一钱包持有客户数码 资产；

- 制定监控措施，以防范及缓解对种子及私人密钥有接达权的获授权人士串通的风险；

- 在办公室以外地方有充足的种子及私人密钥备份及相关应变安排， 并应对有关备份及相关应变安排设有与最初的种子及私人密钥相同的保安监控措施。种子及私人密钥备份应以脱机方式储存于安全的实际地点，而该地点应与最初的种子及私人密钥储存的主要地点不同，且不会受该主要地点发生的任何事件影响；

- 除非另有充足理据，否则应以并无与互联网连接的线下储存方式储存大部分[8]客户数码资产；

- 只容许透过属于客户[9]并列于允许的范围内的钱包地址(例如透过讯息签署测试或微支付测试等拥有权证明测试来核实)存入或提取客户数码资产；

- 实施措施以确保在保管过程中使用的任何智能合约在不存在任何合约隐忧或安全缺失方面达至高可信度；及

- 设有适当的保险／补偿安排[10]，其中包括就认可机构遭黑客攻击的事件、盗窃或欺诈等事项(无论是否因认可机构的行为、错误、遗漏

[8] 如所保管的客户数码资产为虚拟资产，认可机构应以线下储存方式储存 98%的客户数码资产。

[9] 「客户」亦指另一间认可机构或持牌法团在认可机构开立的账户代持有数码资产的客户。

[10] 如所保管的客户数码资产为虚拟资产，认可机构应设有补偿安排或保险，为以线下储存方式及以在线和其他储存方式持有的客户虚拟资产的潜在损失分别提供 50%及 100%的保障。

或严重疏忽所致)而可能产生的客户数码资产的任何损失提供充足保障。

12. 如认可机构为客户提供用户界面或入门网站以管理由认可机构持有的有关客户的资产，认可机构应按照金管局不时发出的相关指引，制定有效的客户认证及通知监控措施。

13. 认可机构应密切监察新保安威胁、漏洞、攻击及欺诈风险与科技解决方案的趋势与发展；因应新威胁及科技发展，定期评估保安风险监控措施的充足度及稳健性；以及制定措施以确保保管客户数码资产技术与相关业内最佳作业手法及适用国际标准相符。用作保管客户数码资产的钱包储存技术应在应用前予以测试以确保可靠性。

(D) 转授与外判

14. 作为一般原则[11]，就虚拟资产而言，认可机构只可将其保管职能转授或外判予：(i)另一间认可机构(或本地注册认可机构的附属公司)；或 (ii)获证券及期货事务监察委员会批给牌照的虚拟资产交易平台[12]。就非虚拟资产的数码资产而言，如属于公有非许可制DLT网络上的非许可制代币，认可机构应格外审慎，严谨地评估是否适合转授权力或外判其保管职能。

15. 如认可机构在提供数码资产保管服务时订立转授或外判安排，应在甄选及委任获转授人或服务提供者前进行适当的尽职审查。认可机构应评估并信纳该获转授人或服务提供者的财政稳健程度、信誉、管理技巧、技术及运作能力、确保符合本附件所载的预期标准及其他适用法律与监管规定的能力、紧贴数码资产方面的技术发展的能力等。认可机构应以文件记录相关尽职审查评估及其结果，并妥善保存。认可机构应设有有效监控措施，以持续监察获转授人或服务提供商的表现。

16. 在提供数码资产保管服务时聘用获转授人或服务提供商，认可机构应具备技术专业知识以评估为保管客户的数码资产所运用的方案的成

[11] 参考证监会于 2023 年 6 月发出适用于虚拟资产交易平台营运者的指引第 X 部分第 10.1 段，以及证监会于 2023 年 12 月 22 日发出有关证监会认可基金投资虚拟资产的通函第 19 段。

[12] 可透过有联系实体持有客户虚拟资产。

效，以及有否引入任何缺失的可能。此外，认可机构应全面了解获转授人或服务提供者持有客户数码资产的条款及条件，并评估会否对客户的法定权利造成重大影响，包括在获转授人或服务提供者一旦无力偿债的情况。认可机构有责任确保获转授人或服务提供者按照本附件第 6 及 7 段所述妥善分隔客户数码资产。

17. 认可机构的应变及灾难复原安排应涵盖转授或外判的数码资产保管服务受中断的情况。认可机构亦应评估获转授人或服务提供商的稳健性，包括其应变计划及程序，以确保保管服务可提供。

18. 此外，认可机构应维持与传统金融服务的转授或外判安排相同的相关系统与监控措施。

19. 认可机构对任何转授或外判活动负有最终责任。

(E) 披露

20. 认可机构应就保管安排以清晰易明的方式向客户作出全面及公平的披露，内容包括：

- 认可机构及其客户各自的权利与责任，包括一旦认可机构无力偿 债或进入处置程序，客户对其资产的拥有权；
- 保管安排，包括如何储存及分隔客户数码资产、存入及提取客户数码资产的程序及所需时间，以及任何适用费用与成本；
- 保险 / 补偿安排以为保安事故或挪用行为等引致的客户数码资产的潜在损失提供保障；
- 任何客户数码资产与其他客户的资产混合的情况及相关风险；
- 认可机构获取客户数码资产的法定及 / 或实益所有权，或以其他方式转移、借出、质押、再质押客户数码资产或对客户数码资产设定任何产权负担的情况与安排，以及相关风险；

- 在发生投票、硬分叉或空投等事件时，对客户数码资产及其相关权利与所有权的处理；及

- 是否有任何与认可机构的保管服务相关的潜在及／或实际利益冲 突，以及该等冲突的性质。

(F) 备存纪录及客户数码资产对帐

21. 认可机构应就每名客户备存簿册及纪录，以追踪及记录客户数码资产的拥有权，包括其对客户负有的资产数量及种类，以及资产进出客户 账户的情况。认可机构应就客户数码资产按每名客户进行定期及频密的对帐，并计及相关的链下及链上纪录。如发现任何差异，应及时处理，并按需要及时上报高级管理层。

22. 认可机构应设有系统及监控措施以备存及保障所有与保管活动有关 的纪录，并应金管局要求时适时提供予金管局。

(G) 打击洗钱及恐怖分子资金筹集

23. 认可机构应确保其打击洗钱及恐怖分子资金筹集(反洗钱)政策、程序 及监控措施能有效管理及缓解与其数码资产保管活动相关的任何洗钱及恐怖分子资金筹集风险。认可机构应遵守《打击洗钱及恐怖分子资金筹集指引（认可机构适用）》及金管局就数码资产保管活动发出的任何反洗钱指引。

(H) 持续监察

24. 认可机构应定期审视其政策及程序，并对其系统与监控措施以及遵守有关保管客户数码资产的适用规定的情况进行独立审计。