(翻譯本)

本局檔號：B1/15C
G16/1C

致：所有認可機構
行政總裁

敬啟者：

提供數碼資產保管服務

隨着數碼資產產業持續發展，香港金融管理局(金管局)留意到認可機構對數碼資產[1]相關活動，尤其為客戶提供數碼資產保管服務的興趣日益濃厚。

為確保認可機構保管的客戶數碼資產得到充分保障，同時相關風險得到妥善管理，金管局認為有需要就認可機構提供數碼資產保管服務提供指引。金管局參考國際標準及做法，制定附件所載的預期標準，並賦予認可機構靈活性，可因應所保管的數碼資產的性質、特點及風險制定相稱的運作安排。認可機構應按照該等標準保障客戶數碼資產，不論認可機構是在以中介人身分進行虛擬資產相關活動[2]、在分銷代幣化產品或是在提供獨立的保管服務的過程中收取該等資產。

除附件所載的預期標準外，認可機構在提供數碼資產保管服務時亦應遵守所有適用法律及監管規定。

本通告適用於進行數碼資產保管活動的認可機構及本地註冊認可機構的附屬公司。本地註冊認可機構應確保該等附屬公司的業務操守、作業方式及監控措施均符合本通告及附件。

---

1 就本通告而言，「數碼資產」一詞指主要依賴加密及分布式分類帳或類似技術的數碼資產，例如《打擊洗錢及恐怖分子資金籌集條例》(《打擊洗錢條例》)第 53ZRA 條所界定的虛擬資產、代幣化證券及其他代幣化資產。此外，「數碼資產」一詞應理解為亦涵蓋接達數碼資產的方式，一般是指私人密鑰、種子或其備份。《打擊洗錢條例》第 53ZR 條所界定的有限用途數碼代幣則不在本通告的涵蓋範圍內。本通告不適用於認可機構或其集團公司保管並非代表客戶持有的自營資產。

2 見金管局與證券及期貨事務監察委員會發出的「有關中介人的虛擬資產相關活動的聯合通函」(最新於 2023 年 12 月 22 日更新)。

實施

如認可機構或(如屬本地註冊認可機構)其附屬公司有意提供數碼資產保管服務，應事先與金管局商討，並向金管局顯示並使其信納它們符合本通告所載的預期標準及規定(及經不時修訂的該等標準及規定)。

如認可機構或本地註冊認可機構的附屬公司已開展數碼資產保管活動，應審視及按需要修訂其系統與監控措施。該等認可機構或其附屬公司已開展數碼資產保管活動的本地註冊認可機構應在本通告日期起計 **6 個月**內通知金管局及確認其已符合附件所載的預期標準。

金管局會密切留意迅速發展的數碼資產市場及國際監管環境，如有需要，可提供進一步指引。貴機構如對本通告有任何問題，請聯絡周佑旌先生(2878-8310)或陳嘉霖女士(2878-1210)。

助理總裁(銀行操守)
區毓麟

2024 年 2 月 20 日

連附件

副本送：證券及期貨事務監察委員會 (收件人：中介機構部臨時主管蔡鍾輝先生)

附件

有關認可機構提供數碼資產保管服務的預期標準的指引

本指引適用於認可機構及本地註冊認可機構的附屬公司[3]代客戶持有的數碼資產(即主要依賴加密及分布式分類帳或類似技術的數碼資產)(下文稱為「客戶數碼資產」)的保管活動，但不包括有限用途數碼代幣[4]。所涵蓋資產包括虛擬資產[5]、代幣化證券及其他代幣化資產[6]。本指引不適用於認可機構或其集團公司保管並非代表客戶持有的自營資產。

(A) 管治及風險管理

1. 認可機構在推出數碼資產保管服務前，應進行全面的風險評估，以識別及了解相關風險。認可機構應在考慮適用的法律及監管規定後，制定適當的政策、程序及監控措施，以管理及緩解所識別的風險。認可機構的董事局及高級管理層應對風險管理過程實施有效監察，以確保在從事保管活動前及持續地識別、評估、管理及緩解與保管活動相關的風險。

2. 認可機構應就其保管活動分配充足資源，包括所需人手及專業知識，以確保妥善的管治、運作及有效的風險管理。高級管理層及負責進行認可機構的保管活動與相關監控職能的職員應具備所需知識、技能及專業知識，以履行其職責。

3. 鑑於數碼資產市場發展迅速，認可機構應確保向高級管理層及參與保管活動的職員提供充足培訓，使其能持續具備勝任能力。

4. 認可機構應就保管活動設有適當的問責安排，包括以書面形式清楚列明角色與責任，以及匯報途徑。認可機構亦應設有充足的政策及程序，

---

[3] 就本附錄其餘部分而言，「認可機構」一詞包括本地註冊認可機構的附屬公司提供數碼資產保管服務。

[4] 如《打擊洗錢條例》第 53ZR 條所界定。

[5] 如《打擊洗錢條例》第 53ZRA 條所界定。

[6] 「代幣化證券」及「其他代幣化資產」一般指以分布式分類帳或類似技術記錄擁有權的數碼形式證券(「證券」定義如《證券及期貨條例》所界定)及數碼形式的其他現實世界資產。

以識別、管理及緩解可能產生的任何潛在及／或實際利益衝突，例如在認可機構或其附屬成員進行的不同活動之間所產生的任何潛在及／或實際利益衝突。

5. 認可機構應制定及維持有效的應變及災難復原安排，以確保其保管活動可持續運作。

(B) 分隔客戶數碼資產

6. 認可機構應在獨立的客戶帳戶[7]持有客戶數碼資產，與認可機構本身的資產分隔，以確保一旦認可機構無力償債或進入處置程序時，能保護客戶數碼資產免受認可機構債權人的申索影響。

7. 認可機構不應轉移客戶數碼資產的任何權利、擁有權、法定及／或實益所有權，或以其他方式借出、質押、再質押客戶數碼資產或對客戶數碼資產設定任何產權負擔，惟以下情況除外：(i)交易的交收，及／或支付客戶欠認可機構的費用及收費；(ii) 事前已取得客戶的明確書面同意；或(iii)法律規定。認可機構應設有充足及有效措施，以防範認可機構為其本身帳戶或為與其客戶商定以外的任何其他目的使用客戶數碼資產。

(C) 保障客戶數碼資產

8. 認可機構應設有充足的系統及監控措施，以確保客戶數碼資產盡快及妥善地加以記帳及獲得充分保障。尤其是，認可機構應設有有效監控措施，以減低因盜竊、欺詐、疏忽或其他挪用行為，以及延誤接達或未能接達客戶數碼資產而導致客戶數碼資產有任何損失的風險。

9. 認可機構可採取風險為本方法，因應所保管的數碼資產的性質、特點及風險，制定系統與監控措施以保障客戶數碼資產。舉例來說，風險會視乎所用的分布式分類帳技術(DLT)網絡(例如私有許可制、公有許可制及公有非許可制)，以及所設立的緩解措施。例如與設有 DLT 網

[7] 包括於分布式分類帳持有客戶數碼資產的錢包地址，而有關錢包地址應與用作持有認可機構本身資產的錢包地址分隔。

絡接達權限制的公有許可制及私有許可制 DLT 網絡相比，於公有非許可制 DLT 網絡以非許可制代幣形式持有客戶數碼資產，可能會面對更高的網絡保安風險，亦可能於發生盜竊、黑客入侵或其他網絡攻擊後，難以追回所失去的資產。

10. 保障客戶數碼資產的系統與監控措施包括有關以下各方面的書面政策及程序等：

- 授權及核實以進行客戶數碼資產存入、提取及轉移的接達，包括儲存種子及私人密鑰的裝置的接達；及

- 管理及保障客戶數碼資產的種子及私人密鑰，範圍涵蓋密鑰的產生、分派、儲存、使用、銷毀及備份。

11. 尤其是，認可機構應採納相關業內最佳作業手法，並遵循適用國際保安標準，以與所持有資產的性質、特點及風險相稱的方式保障客戶數碼資產。儘管下述程序及監控措施不擬作為硬性規定或適用於所有情況，但若認可機構持有客戶虛擬資產，一般都必須實施該等程序及監控措施。就其他數碼資產而言，認可機構可採用風險為本方法，按與所造成的風險相稱的方式實施下述程序及監控措施；惟如該數碼資產屬於公有非許可制 DLT 網絡上的非許可制代幣，認可機構應格外審慎，嚴謹地評估以下程序及監控措施的實施：

- 在安全及防竄改的環境及裝置(例如以硬件安全模組(Hardware Security Module)，簡稱 HSM)中產生及儲存種子及私人密鑰，包括其備份。在實際可行情況下，應以離線方式產生種子及私人密鑰，並設有適當的生命周期上限；

- 在香港以安全的方式產生、儲存及備份種子及私人密鑰；

- 按有需要知道的基礎，嚴格限制對加密裝置或應用程式的存取，只限經適當甄選及培訓的獲授權人士進行；備存最新的文件，以記錄如何授權及核實接達權，以及如何分配接達權；使用可靠有力的認證方法(如多重認證)確認對種子及私人密鑰的接達權；備存有關接達加密裝置或應用程式的審計線索；

- 實施穩健的監控措施，以避免出現任何缺失的可能，例如藉利用密鑰分片或類似技術分拆及分散私人密鑰，在認可機構授權的多名人員之間進行分散儲存，從而並無單一人士可持有有關密鑰的完整資料。在一般情況下，一定數目的密鑰分片持有人須集體行事，共同簽訂一項交易，以確保並無單一人士可管有完整的接達權，並可同時防範因某一分片遺失、無法取得或被盜而令運作中斷。為防範出現缺失的可能，亦可考慮使用多個錢包而非單一錢包持有客戶數碼資產；

- 制定監控措施，以防範及緩解對種子及私人密鑰有接達權的獲授權人士串通的風險；

- 在辦公室以外地方有充足的種子及私人密鑰備份及相關應變安排，並應對有關備份及相關應變安排設有與最初的種子及私人密鑰相同的保安監控措施。種子及私人密鑰備份應以離線方式儲存於安全的實際地點，而該地點應與最初的種子及私人密鑰儲存的主要地點不同，且不會受該主要地點發生的任何事件影響；

- 除非另有充足理據，否則應以並無與互聯網連接的線下儲存方式儲存大部分[8]客戶數碼資產；

- 只容許透過屬於客戶[9]並列於允許的範圍內的錢包地址(例如透過訊息簽署測試或微支付測試等擁有權證明測試來核實)存入或提取客戶數碼資產；

- 實施措施以確保在保管過程中使用的任何智能合約在不存在任何合約隱憂或安全缺失方面達至高可信度；及

- 設有適當的保險／補償安排[10]，其中包括就認可機構遭黑客攻擊的事件、盜竊或欺詐等事項(無論是否因認可機構的行為、錯誤、遺漏

[8] 如所保管的客戶數碼資產為虛擬資產，認可機構應以線下儲存方式儲存 98%的客戶數碼資產。

[9] 「客戶」亦指另一間認可機構或持牌法團在認可機構開立的帳戶代持有數碼資產的客戶。

[10] 如所保管的客戶數碼資產為虛擬資產，認可機構應設有補償安排或保險，為以線下儲存方式及以線上和其他儲存方式持有的客戶虛擬資產的潛在損失分別提供 50%及 100%的保障。

或嚴重疏忽所致)而可能產生的客戶數碼資產的任何損失提供充足保障。

12. 如認可機構為客戶提供用戶界面或入門網站以管理由認可機構持有的有關客戶的資產，認可機構應按照金管局不時發出的相關指引，制定有效的客戶認證及通知監控措施。

13. 認可機構應密切監察新保安威脅、漏洞、攻擊及欺詐風險與科技解決方案的趨勢與發展；因應新威脅及科技發展，定期評估保安風險監控措施的充足度及穩健性；以及制定措施以確保保管客戶數碼資產技術與相關業內最佳作業手法及適用國際標準相符。用作保管客戶數碼資產的錢包儲存技術應在應用前予以測試以確保可靠性。

(D) 轉授與外判

14. 作為一般原則[11]，就虛擬資產而言，認可機構只可將其保管職能轉授或外判予：(i)另一間認可機構(或本地註冊認可機構的附屬公司)；或(ii)獲證券及期貨事務監察委員會批給牌照的虛擬資產交易平台[12]。就非虛擬資產的數碼資產而言，如屬於公有非許可制 DLT 網絡上的非許可制代幣，認可機構應格外審慎，嚴謹地評估是否適合轉授權力或外判其保管職能。

15. 如認可機構在提供數碼資產保管服務時訂立轉授或外判安排，應在甄選及委任獲轉授人或服務提供者前進行適當的盡職審查。認可機構應評估並信納該獲轉授人或服務提供者的財政穩健程度、信譽、管理技巧、技術及運作能力、確保符合本附件所載的預期標準及其他適用法律與監管規定的能力、緊貼數碼資產方面的技術發展的能力等。認可機構應以文件記錄相關盡職審查評估及其結果，並妥善保存。認可機構應設有有效監控措施，以持續監察獲轉授人或服務提供者的表現。

16. 在提供數碼資產保管服務時聘用獲轉授人或服務提供者，認可機構應具備技術專業知識以評估為保管客戶的數碼資產所運用的方案的成

[11] 參考證監會於 2023 年 6 月發出適用於虛擬資產交易平台營運者的指引第 X 部分第 10.1 段，以及證監會於 2023 年 12 月 22 日發出有關證監會認可基金投資虛擬資產的通函第 19 段。

[12] 可透過有聯繫實體持有客戶虛擬資產。

效，以及有否引入任何缺失的可能。此外，認可機構應全面了解獲轉授人或服務提供者持有客戶數碼資產的條款及條件，並評估會否對客戶的法定權利造成重大影響，包括在獲轉授人或服務提供者一旦無力償債的情況。認可機構有責任確保獲轉授人或服務提供者按照本附件第 6 及 7 段所述妥善分隔客戶數碼資產。

17. 認可機構的應變及災難復原安排應涵蓋轉授或外判的數碼資產保管服務受中斷的情況。認可機構亦應評估獲轉授人或服務提供者的穩健性，包括其應變計劃及程序，以確保保管服務可提供。

18. 此外，認可機構應維持與傳統金融服務的轉授或外判安排相同的相關系統與監控措施。

19. 認可機構對任何轉授或外判活動負有最終責任。

(E) 披露

20. 認可機構應就保管安排以清晰易明的方式向客戶作出全面及公平的披露，內容包括：

- 認可機構及其客戶各自的權利與責任，包括一旦認可機構無力償債或進入處置程序，客戶對其資產的擁有權；
- 保管安排，包括如何儲存及分隔客戶數碼資產、存入及提取客戶數碼資產的程序及所需時間，以及任何適用費用與成本；
- 保險／補償安排以為保安事故或挪用行為等引致的客戶數碼資產的潛在損失提供保障；
- 任何客戶數碼資產與其他客戶的資產混合的情況及相關風險；
- 認可機構獲取客戶數碼資產的法定及／或實益所有權，或以其他方式轉移、借出、質押、再質押客戶數碼資產或對客戶數碼資產設定任何產權負擔的情況與安排，以及相關風險；

- 在發生投票、硬分叉或空投等事件時，對客戶數碼資產及其相關權利與所有權的處理；及

- 是否有任何與認可機構的保管服務相關的潛在及／或實際利益衝突，以及該等衝突的性質。

(F) 備存紀錄及客戶數碼資產對帳

21. 認可機構應就每名客戶備存簿冊及紀錄，以追踪及記錄客戶數碼資產的擁有權，包括其對客戶負有的資產數量及種類，以及資產進出客戶帳戶的情況。認可機構應就客戶數碼資產按每名客戶進行定期及頻密的對帳，並計及相關的鏈下及鏈上紀錄。如發現任何差異，應及時處理，並按需要及時上報高級管理層。

22. 認可機構應設有系統及監控措施以備存及保障所有與保管活動有關的紀錄，並應金管局要求時適時提供予金管局。

(G) 打擊洗錢及恐怖分子資金籌集

23. 認可機構應確保其打擊洗錢及恐怖分子資金籌集(反洗錢)政策、程序及監控措施能有效管理及緩解與其數碼資產保管活動相關的任何洗錢及恐怖分子資金籌集風險。認可機構應遵守《打擊洗錢及恐怖分子資金籌集指引（認可機構適用）》及金管局就數碼資產保管活動發出的任何反洗錢指引。

(H) 持續監察

24. 認可機構應定期審視其政策及程序，並對其系統與監控措施以及遵守有關保管客戶數碼資產的適用規定的情況進行獨立審計。