cmta.

Standard pour la conservation d'actifs digitaux

Mars 2023

Standard pour la conservation d'actifs digitaux

Version: 2.0
Adopté: 1er mars 2023

Capital Markets and Technology Association
Route de Chêne 30
1208 Genève

admin@cmta.ch
+41 22 318 73 13

Table of contents

1. INTRODUCTION

§ 1.1 CONTEXTE

La Capital Markets and Technology Association (**CMTA**) est une association suisse indépendante qui réunit des experts des secteurs financier, technologique, juridique et de la révision pour promouvoir l'utilisation des nouvelles technologies dans les marchés des capitaux. La CMTA offre une plateforme pour la création de standards ouverts et généralement acceptés par l'industrie financière concernant l'émission, la distribution et la négociation de valeurs mobilières et d'autres instruments financiers sous forme d'actifs digitaux au moyen de la technologie des registres distribués (**TRD**).

Ce document définit le standard de la CMTA en matière de conservation d'actifs digitaux (*Digital Assets Custody Standard* ou **DACS**); il énonce des exigences et des recommandations (**E&R**) pour les solutions technologiques tendant à la conservation et à la gestion des actifs digitaux.

Le DACS tend à promouvoir un niveau d'assurance élevé pour les propriétaires d'actifs digitaux, sans pour autant indûment entraver les activités des prestataires de services ou les possibilités d'utilisation du système. Sur le plan opérationnel et de la sécurité, la conservation des actifs digitaux se distingue de celle des actifs financiers traditionnels. Ces particularités sont source de défis pour les prestataires de services concernés, les plus notables étant de pouvoir générer, utiliser et conserver des clés privées (**CP**) se rapportant aux actifs digitaux de façon sécurisée tout au long du processus de conservation de ces actifs.

Le DACS fournit un point de référence aux clients et aux réviseurs pour évaluer une solution de conservation ou un prestataire de service. Dans cette perspective, les E&R du DACS sont conçues et énoncées de façon à être dans la mesure du possible fondées sur des bases objectives, susceptibles d'être vérifiés par des tiers, et indépendantes des modes de mise en œuvre et des types d'actifs. La liste des E&R du DACS n'a pas vocation à être limitative.

Les principes directeurs du DACS sont la sécurité, la fiabilité, ainsi que la transparence et la maîtrise de la technologie et des processus de conservation. Les E&R ont été énoncées au terme d'un processus de catégorisation et de hiérarchisation auquel se sont associés des contributeurs et évaluateurs issus de plusieurs entreprises qui élaborent et utilisent des solutions technologiques de conservation.

§ 1.2 CHAMP D'APPLICATION

Une solution de conservation d'actifs digitaux requiert la mise en place de procédures permettant de générer des secrets, d'effectuer des calculs au moyen de ces secrets – y compris la création de signatures de transactions – ainsi que de certaines processus et procédures de sécurité pour éviter le vol ou la perte définitive d'actifs. Dans le contexte des actifs digitaux, les éléments suivants peuvent être considérés comme des secrets: les semences (*seeds* ou "clés maîtresses") à partir desquelles les adresses et les paires de clés sont générées, et les CPs d'adresses individuelles. Un système de conservation d'actifs digitaux peut comporter des composants de logiciel et de matériel physique et fonctionne, au moins en partie, par des actions manuelles.

Le DACS classe les E&R d'une solution de conservation en cinq catégories, qui sont elles-mêmes regroupées en deux volets:

A. Volet opérationnel:

    1. choix du modèle de conservation; et

2. fonctionnement technique de la solution de conservation.

B. Volet d'infrastructure:

1. génération de secrets;
2. récupération de secrets; et
3. développement et maintenance.

Les E&R du volet opérationnel concernent les fournisseurs de solutions de conservation d'actifs digitaux. Un fournisseur de solution de conservation se distingue d'un fournisseur de solution d'infrastructure. Ce dernier fournit l'infrastructure nécessaire à la conservation des actifs digitaux, mais ne participe pas à son exploitation. Les aspects de sécurité des E&R du volet d'infrastructure concernent le fournisseur et (s'il est différent) l'exploitant de la solution de conservation. Les E&R peuvent être de nature technique, procédurale ou se rapporter à une combinaison des deux. Le DACS a vocation à être mis à jour et complété régulièrement pour tenir compte des différentes solutions qui apparaissent et qui sont portées à l'attention de la CMTA.

Parmi les aspects potentiellement critiques qui sont le plus souvent exclus du champ d'application du DACS figurent les questions de sécurité procédurale et physique, la sécurité des composants informatiques et des logiciels sous-jacents, la sécurité des composants du matériel, ainsi que les questions de traçabilité et de responsabilité. Le champ d'application du DACS se limite ainsi aux éléments qui sont spécifiques aux solutions de conservation d'actifs digitaux.

Le DACS n'aborde pas les implications juridiques ou réglementaires que peuvent avoir le choix d'un modèle de conservation particulier, ou les implications de l'offre d'un service de conservation particulier. Selon le modèle de conservation d'actifs digitaux retenu, le fournisseur de service peut devoir obtenir une autorisation de la part des autorités, par exemple s'il a le pouvoir de disposer des actifs digitaux conservés et/ou s'il détient les actifs digitaux pour le compte de clients. Le DACS n'a pas vocation à s'appliquer à des services qui ne comportent pas d'élément de conservation (*non-custodial solutions*).

§ 1.3 Certification

La CMTA a établi un régime de certification pour permettre aux entreprises qui utilisent une solution de conservation de faire vérifier qu'elles satisfont aux exigences du DACS. Ces vérifications sont réalisées par des sociétés de révision reconnues et donnent lieu à un rapport formel. Elles évaluent la conformité des contrôles de sécurité mis en œuvre avec certaines exigences et recommandations du DACS.

Le processus de certification du DACS fait l'objet de documents séparés.

§ 1.4 Avertissement

La seule adhésion au DACS ne permet pas de garantir la sécurité d'une solution de conservation, et encore moins celle de son utilisation, car chaque solution de conservation et chaque environnement de mise en œuvre génère inévitablement des vecteurs d'attaque propres. La conservation d'actifs digitaux nécessite l'utilisation de nombreux composants techniques et procéduraux. Elle suppose une confiance placée dans certains composants technologiques ainsi que dans les personnes qui en assurent le fonctionnement. Cela contraste avec les certifications de sécurité qui peuvent être obtenues pour des éléments de matériel (comme par exemple les Common Criteria ou FIPS 140-2 et 140-3), pour lesquels la sécurité peut être plus facilement caractérisée. Il incombe donc à chaque entreprise d'intégrer correctement le DACS dans son processus de gestion des risques. De même, le DACS ne couvre pas tous les facteurs de risque liés à

la conservation d'actifs digitaux. Par exemple, le DACS ne traite pas des questions de connectivité de la blockchain, de gestion du "gaz" ou de gouvernance des contrats intelligents.

§ 1.5 Termes techniques | Définitions

Un glossaire des termes techniques et des termes initialisés qui sont utilisés dans ce document figure à l'**annexe A**.

§ 1.6 Révisions, compléments et mises à jour

Bien que le DACS tende à la neutralité technologique dans toute la mesure du possible, il doit être orienté vers la pratique. La CMTA peut donc périodiquement faire et publier des révisions, des compléments ou des mises à jour.

Tout commentaire ou suggestion concernant d'éventuelles futures mises à jour du DACS peuvent être adressés au Secrétariat de la CMTA par courrier électronique à l'adresse admin@cmta.ch.

2. MODÈLES DE CONSERVATION

§ 2.1 Introduction

Les banques et autres établissements financiers peuvent exploiter des solutions d'auto-conservation (*self-custody*), dans le cadre desquelles une solution technologique est conçue, construite, contrôlée et exploitée par l'établissement de façon à lui permettre de gérer lui-même des adresses du registre distribué (**ADR**). Les différents modèles de gestion des ADR et leurs caractéristiques sont décrits à la section suivante.

Toute organisation n'est pas en mesure de développer, entretenir et exploiter une infrastructure d'auto-conservation pour actifs digitaux. Les investisseurs institutionnels tels que les organismes de placements collectifs ou les gestionnaires de fortune ont généralement une obligation légale de travailler avec des dépositaires tiers ou des prestataires de services d'infrastructure répondant à certaines exigences lorsqu'ils traitent les actifs de clients. L'auto-conservation n'est dès lors souvent pas une option viable pour de tels établissements.

Les établissements financiers doivent connaître les organisations qui conservent les actifs digitaux de leurs clients. Elles doivent notamment savoir comment ce dépositaire protège les secrets et l'intégrité des secrets cryptographiques, en particulier les CP.

§ 2.2 Types de modèles de conservation

Les actifs digitaux peuvent être conservés par un intermédiaire selon différents modèles, dont chacun a ses propres caractéristiques, particularités et limitations. La plupart des solutions disponibles peuvent être rangées dans l'un des types de modèles ci-dessous.

Modèle	Description	Allocation	Modèle
ADR groupées	Détention groupée des actifs digitaux des clients (mais des clients seulement) sur une ou plusieurs ADR	Attribution au niveau des clients – Un registre interne du dépositaire attribue les actifs digitaux pertinents aux différents clients (mais les actifs digitaux ne sont pas enregistrés sur des ADR distinctes; pas d'attribution sur le registre distribué lui-même).	1
		Attribution au niveau de l'ADR – Un registre interne attribue les actifs digitaux inscrits sur chaque ADR à des clients spécifiques (des actifs digitaux pouvant être détenus pour plusieurs clients sur plusieurs ADR) au niveau du dépositaire (pas d'attribution sur le registre distribué lui-même).	2
	Détention groupée des actifs digitaux détenus pour compte propre et pour le compte de clients sur une ou plusieurs ADR	Mêmes options d'allocation que dans les modèles 1 et 2, mais le dépositaire regroupe les actifs digitaux détenus pour son propre compte avec ceux qu'il détient pour le compte de ses clients.	1P / 2P
ADR dédiées	Une ou plusieurs ADR sont attribuées à chaque client (mais aucune ADR n'est attribuée à plus d'un client)	Un registre interne attribue chaque ADR à un client déterminé.	3
Conservation déléguée	Les actifs digitaux sont déposés auprès d'un sous-dépositaire tiers	Les actifs détenus auprès du sous-dépositaire sont identifiés au niveau du dépositaire (registre interne); différents modèles sont possibles au niveau sous-dépositaire, selon notamment la juridiction concernée (voir les modèles 1 à 3 ci-dessus).	4
ADR privées	Une ou plusieurs ADR sont attribuées à chaque client et la CP est contrôlée par le client exclusivement	Il s'agit d'un modèle de détention sans conservation (*non-custodial solution*) où aucun service de conservation n'est fourni.	5

Le choix d'un modèle de conservation a des implications juridiques, techniques et comptables en ce qui concerne le stockage et le traitement des actifs digitaux concernés.

Ces conséquences peuvent notamment dépendre:

A. de la qualification juridique et de la nature des actifs digitaux détenus (tels que les crypto-monnaies, créances, valeurs mobilières ou autres instruments financiers), ainsi que:

B. du statut juridique du dépositaire (*e.g.* banque, maison de titres ou dépositaire non réglementé).

Il est postulé ici que, pour les modèles de conservation 1 à 3, les CP de chaque ADR sont contrôlées par le dépositaire (ou le sous-dépositaire) exclusivement, et cela alors même que des modèles de contrôle partagé des CP soient possible et soient utilisés en pratique pour des mises en œuvre d'infrastructures de conservation comparables au modèle 3 (c'est-à-dire dans lesquelles le client dispose d'un certain degré de contrôle sur les CP, mais pas d'un contrôle exclusif).

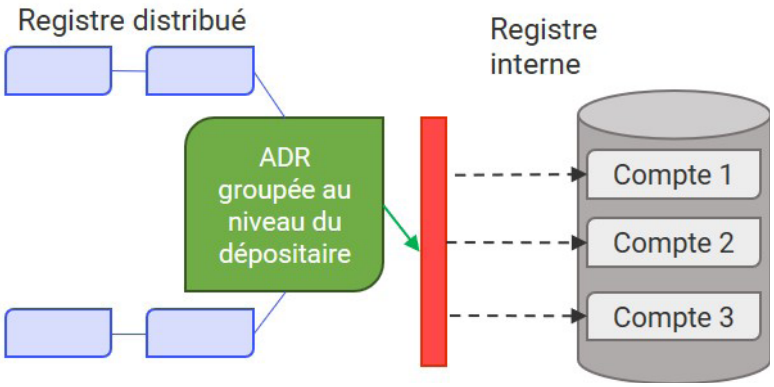
Les modèles 4 et 5 n'impliquent pas de conservation de CP par le prestataire de services, voire pas de conservation du

tout (modèle 5). Ces modèles sont mentionnés ici pour mémoire et ne sont pas traités plus avant ici.

Les modèles 1 à 3 (qui impliquent des opérations de conservation d'actifs digitaux) peuvent être décrits comme il suit:

2.2.1 Modèle 1

Dans ce modèle d'ADR groupées, les actifs digitaux sont conservés sur des ADR créées et contrôlées par le dépositaire. Les CP correspondant aux ADR sont contrôlées par le dépositaire exclusivement.



Le dépositaire tient un registre interne pour suivre les inscriptions faites sur les différentes ADR et faire correspondre les inscriptions et le solde des ADR avec les comptes de dépôt des clients. En particulier, le registre interne identifie les actifs digitaux détenus de façon groupée pour chaque client (allocation au sein du groupe) ainsi que du solde du compte de chaque client. Le dépositaire attribue les actifs digitaux à chaque client dans le registre interne, qui s'intègre dans le système de comptabilité client du dépositaire. Il n'existe cependant pas de lien spécifique ou d'attribution d'une ADR particulière et/ou de certains actifs digitaux spécifiques à un client particulier. Cela signifie que l'attribution des soldes d'actifs digitaux aux clients n'existe que dans le registre interne, mais pas dans les ADR du dépositaire.

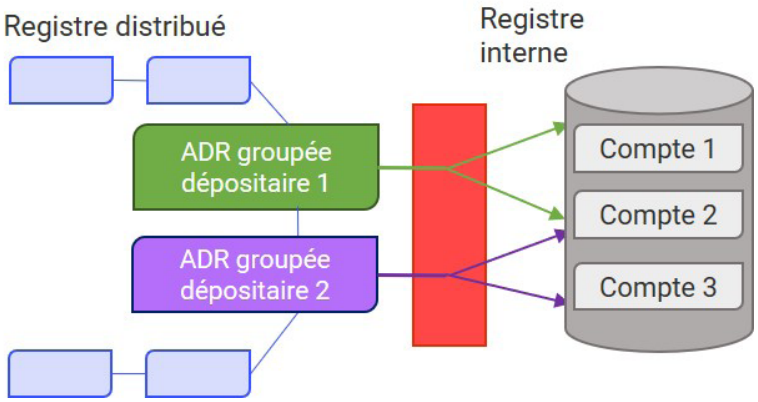
L'allocation faite au niveau du groupe peut s'étendre aux actifs digitaux que le dépositaire conserve auprès de sous-dépositaires, de façon à ce que le registre interne couvre à la fois les ADR groupées du modèle 1 et les positions détenues auprès de sous-dépositaires (modèle 4).

Ce modèle est similaire à celui que les banques et les maisons de titres utilisent pour les instruments financiers de leurs clients lorsque plusieurs sous-dépositaires (ou plusieurs comptes tenus auprès d'un même sous-dépositaire) sont utilisés pour le même instrument financier. En pratique, pour des raisons opérationnelles, la conservation d'actifs digitaux se fait généralement plutôt conformément au modèle 2 (voir ci-dessous).

2.2.2 Modèle 2

Dans le modèle de regroupement de type 2, les actifs digitaux sont conservés sur des ADR créées et contrôlées par le dépositaire. Les CP correspondantes sont contrôlées exclusivement par le dépositaire. Tant le modèle 2 que le modèle 1 supposent un groupement. L'élément distinctif est que, dans le modèle 2, le registre interne attribue les actifs digitaux inscrits sur chaque ADR à un ou plusieurs clients (attribution au niveau de l'ADR), plutôt que de procéder à une attribution globale comme c'est le cas dans le modèle 1.

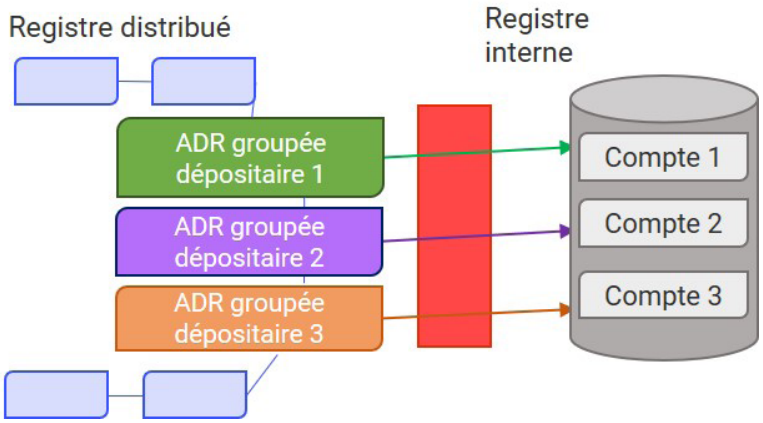
Les modèles 1 et 2 sont en pratique identiques lorsque le dépositaire utilise une ADR groupée unique pour chaque type d'actif digital.



Ce modèle est similaire à celui que les banques et les maisons de titres utilisent pour les instruments financiers de leurs clients lorsque le dépositaire fait appel à un sous-dépositaire distinct pour chaque instrument financier (ou type d'instrument financier) ou à des comptes groupés auprès d'un même sous-dépositaire (par exemple, des comptes groupés détenus par une banque ou une maison de titres suisse auprès d'un dépositaire central américain).

2.2.3 Modèle 3

Dans ce modèle le registre interne du dépositaire attribue chaque ADR que ce dernier contrôle à un client unique; il n'y a pas de regroupement des actifs de plusieurs clients et un lien direct peut être établi entre chaque ADR et le compte du client. Les CP sont soit contrôlées par le dépositaire exclusivement, soit partagées entre le dépositaire et le client. Tel peut être le cas lorsque des systèmes de signature à seuil ou impliquant d'autres méthodes de calcul multipartites (*threshold signature schemes* ou *multiparty computation methods*) sont utilisés (voir le § 2.3 ci-dessous).



§ 2.3 Implications du choix d'un modèle de conservation

Le choix d'un ou de plusieurs des modèles de conservation décrits ci-dessus peut avoir des implications juridiques et réglementaires selon le type d'actif digital et le statut réglementaire du prestataire de service concerné. Le DACS ne traite pas de ces questions. Chaque dépositaire doit identifier le ou les modèles les plus adaptés à son offre de services et à son statut réglementaire propre.

D'autres modèles que ceux décrits dans ce document sont envisageables, comme par exemple des modèles qui impliquent un contrôle partagé d'une ADR ou d'une CP au moyen de signatures multiples, multipartites, globales ou à seuils et/ou d'autres méthodes de calcul multipartites (**MPC**). Dans de telles situations, il se peut qu'aucune entité

ou personne n'ait le contrôle exclusif des ADR ou CP correspondantes, et ne soit donc "dépositaire" des actifs digitaux concernés au sens de ce document. Ces modèles sont parfois désignés par le terme de "conservation partielle".

Le DACS est en principe indifférent au modèle de conservation choisi, dans la mesure où, dans son itération actuelle, ses E&R portent en premier lieu sur des questions de sécurité.

3. DACS – EXIGENCES ET RECOMMENDATIONS

Cette section énumère les exigences et recommandations (E&R) du DACS. Celles-ci doivent être mises en œuvre en considérant la technologie utilisée dans les organisations concernées, le contexte dans lequel les services sont rendus, ainsi que les documents de support disponibles. Ces E&R ont vocation à s'appliquer à toute solution de conservation viable, indépendamment de leurs éléments spécifiques. Une exigence ou une recommandation particulière peut néanmoins s'avérer inapplicable dans un cas particulier. Les activités décrites dans les exigences et les recommandations doivent être menées par des parties disposant de l'expertise et des compétences nécessaires.

Les E&R sont divisées en deux catégories: opérations et infrastructure. Le volet "opérations" ne concerne que l'opérateur d'une solution de conservation, tandis que le volet "infrastructure" concerne à la fois l'opérateur et (s'il est différent) le prestataire de services qui fournit l'infrastructure. Ainsi, si un établissement financier choisit un prestataire pour lui fournir une infrastructure de conservation d'actifs digitaux qu'il entend exploiter lui-même, l'établissement financier est responsable du respect des E&R relatives au volet opérationnel, alors que le fournisseur doit pouvoir démontrer que la solution d'infrastructure satisfait aux E&R du volet "infrastructure".

VOLET OPÉRATIONNEL

§ 3.1 CHOIX DU MODÈLE DE CONSERVATION

Cette section énonce les principes essentiels à appliquer lorsque l'opérateur détermine le type de modèle de conservation à adopter. Bien que cette section ne s'applique pas aux fournisseurs de solutions d'infrastructure qui ne sont pas impliqués dans l'exploitation de ces dernières, il est tout de même attendu que les prestataires concernés soient en mesure d'indiquer les modèles de conservation que leur solution peut prendre en charge, ainsi que les restrictions opérationnelles qui y sont liées.

3.1.1 Exigences

MOD-00: Les modèles de conservation disponibles pour un registre distribué spécifique sont examinés en fonction de la stratégie et des besoins du prestataire des services de conservation. Le modèle potentiel est évalué par le prestataire des services de conservation en termes de risque commercial, de sécurité et d'aptitude opérationnelle; cet examen est documenté. A titre d'exemple, la documentation peut établir que le modèle de conservation choisi reflète la structure des activités du prestataire de services concerné ainsi que la nature et les attentes de sa clientèle.

MOD-01: Les prestataires de services tiers auxquels tout ou partie des opérations de conservation sont déléguées doivent se conformer au DACS. Sauf indication contraire, c'est généralement à la partie qui externalise qu'il incombe de veiller à ce que cette conformité soit assurée.

3.1.2 Recommendations

MOD-02: Les résultats de l'évaluation des modèles de conservation sont examinés et mis à jour au moins une fois par an et, en tout état de cause, avant le lancement de nouveaux services.

MOD-03: S'ils confient la conservation d'actifs à un tiers, les établissements financiers veillent à ce que tout fournisseur d'infrastructure fasse l'objet d'évaluations périodiques en matière de sécurité (par exemple au moyen d'audits de conformité et de tests de pénétration). Le rapport d'audit est examiné et évalué au regard des systèmes de contrôle des risques de l'organisation concernée.

§ 3.2 Opérations techniques

Cette section couvre les questions liées à l'exploitation d'une solution de conservation par ses utilisateurs finaux. Elle n'est pas directement pertinente pour un prestataire de services (vendeur) qui ne fournit qu'une infrastructure de conservation sans être impliqué dans son exploitation.

3.2.1 Exigences

OPS-00: Un modèle d'identification des menaces adapté à l'organisation est établi. Ce dernier documente les risques et les caractérise par des indicateurs usuels tels que la probabilité de leur occurrence et l'importance de leur impact éventuel. Il détaille les stratégies d'atténuation de ces risques.

OPS-01: Les éléments de logiciels et les services critiques utilisés pour les opérations sont identifiés, évalués et régulièrement mis à jour.

OPS-02: Les éléments de matériel (*hardware*) critiques utilisés pour les opérations sont identifiés et régulièrement mis à jour. Dans la mesure du possible, des certifications externes sont obtenues pour garantir la conformité aux normes, par exemple celles établies par le NIST (FIPS 140-3).

OPS-03: Les valeurs secrètes qui permettent de réaliser des opérations critiques (telles que les semences, les CP pour la signature des transactions ou les jetons d'authentification critiques) sont stockées et utilisées dans un environnement où des contrôles de sécurité sont réalisés pour empêcher des extractions non autorisées. Une exception peut être faite lorsque les valeurs secrètes sont distribuées par des moyens cryptographiques tels que des signatures à seuil ou d'autres types de partage de secret.

La protection des secrets conformément à l'OPS-03 est généralement assurée par l'utilisation d'un composant garantissant l'isolation physique et logique de ces secrets et des calculs qui les concernent. Les solutions adéquates peuvent inclure (sans être limitées à) des modules de sécurité dédiés (hardware security module devices), des systèmes basés sur des cartes à puce ou des environnements d'exécution sécurisés de serveurs, d'ordinateurs personnels ou d'appareils mobiles.

OPS-04: L'accès à l'interface de la solution de conservation est protégé par des listes de contrôle d'accès individuelles et requiert une authentification pour chaque session. Cela s'applique tant à l'interface utilisateur graphique qu'aux interfaces de programmation d'applications (**API**). Les droits d'accès sont revus régulièrement et les droits d'accès qui ne sont plus nécessaires sont révoqués.

OPS-05: L'accès aux fonctions d'administration de la solution et de ses composants (matériel et logiciel) est limité à un nombre minimal de personnes (et n'est donc pas ouvert à quiconque); les droits d'administration des utilisateurs sont examinés régulièrement pour en vérifier l'exactitude et la conformité avec le modèle de risque de l'organisation. Les droits d'accès sont révoqués lorsqu'ils ne sont plus nécessaires. Des mesures

sont prises pour garantir qu'aucune personne ne contrôle seule des fonctions ou des composants de logiciel/ matériel critiques.

OPS-06: L'exécution de transactions ou d'opérations (autres que les transactions ou opérations insignifiantes) nécessite l'approbation d'au moins deux parties indépendantes l'une de l'autre. Dans la mesure du possible, les approbateurs appartiennent à des lignes d'activité différentes. Pour éviter que des parties non autorisées deviennent des approbateurs, l'intégration d'une nouvelle partie approbatrice requiert l'examen et l'approbation de plusieurs parties.

OPS-07: Toutes les communications de réseau réalisées sur des réseaux potentiellement non fiables sont protégées par des moyens cryptographiques et sont mutuellement authentifiées, en utilisant par exemple le protocole TLS ou une autre technologie mettant en œuvre un canal sécurisé, avec une configuration appropriée.

Il est à noter que cette OPS-07 peut ne pas être réalisable à la périphérie du système, si les transactions sont envoyées à un réseau sans autorisation qui, par définition, ne nécessite pas d'authentification autre que la signature des transactions.

OPS-08: Les composants logiciels ou matériels stockant de façon permanente des valeurs secrètes suffisantes pour effectuer des opérations critiques (telles que les semences, les CP pour la signature des transactions ou les jetons d'authentification critiques) ne sont pas orientés vers l'internet, mais peuvent se trouver sur un réseau interne où ils ne sont accessibles qu'après que des contrôles de sécurité appropriés (typiquement une authentification et une autorisation) ont été effectués par un autre système.

OPS-09: Toutes les opérations importantes sont enregistrées et les journaux d'opérations sont conservés suffisamment longtemps pour permettre leur examen pour la recherche d'activités suspectes.

OPS-10: Un processus est défini pour créer une preuve de réserve (*proof-of-reserve*, **PoR**) pour tout ou partie des actifs digitaux conservés. Cette PoR vise à prouver de manière incontestable l'existence de fonds et à établir la propriété des clés liées à un compte d'actifs digitaux spécifique ou à un groupe de comptes. Une PoR peut notamment être obtenue par la réalisation de microtransactions ("test Satoshi") ou d'un système de signature de messages (conçu de façon à ne pas pouvoir être utilisé de manière abusive pour la signature de transactions).

OPS-11: Des contrôles de sécurité techniques sont réalisés pour détecter les activités techniquement suspectes et prévenir les abus, les fraudes et la compromission de la solution. Ces contrôles peuvent comprendre l'établissement de listes d'adresses autorisées ou proscrites (*whitelist/blacklist rules*), des limitations de débit, la mise en œuvre de régimes d'heures autorisées, de verrouillages/réinitialisations automatiques, de verrouillage horaire, etc.

OPS-12: Les antécédents pénaux du personnel impliqué dans la détention de tout ou partie de secrets ou dans l'opération d'une plateforme de services de conservation sont vérifiés sans qu'aucune inscription pertinente ne soit constatée. Le personnel reçoit une formation et est apte et compétent pour exercer sa fonction. La conformité à l'OPS-12 doit être réévaluée régulièrement (en principe chaque année).

OPS-13: Si des clés secrètes (ou des éléments de telles clés) sont stockés sur des supports externes, un inventaire documentant le contenu et l'emplacement des supports de stockage est établi par le dépositaire des actifs (et donc potentiellement par un sous-dépositaire). Cet inventaire est conservé en lieu sûr à des fins d'audit.

OPS-14: Les opérateurs de plateformes de conservation sont responsables de la conduite d'une *due diligence* sur les nouveaux clients. Si les clients souhaitent transférer leurs propres actifs digitaux dans le système de l'opérateur, une vérification préalable de la blockchain doit être effectuée, comportant une analyse des portefeuilles du client et des dernières transactions réalisées. Cela contribue au respect des règles applicables en matière d'identification des clients (*KYC*) et de lutte contre le blanchiment d'argent.

OPS-15: Chacune des parties concernées a adopté et applique des politiques concernant la gestion des changements, la gestion des accès, la gestion des vulnérabilités et la gestion des correctifs, qui couvrent la solution de conservation et son environnement.

OPS-16: Les composants de logiciel critiques de la solution de conservation visés à l'OPS-01 sont évalués au moins une fois par an par des spécialistes externes indépendants en termes de fiabilité et de sécurité. Ces évaluations doivent comprendre des audits du code source et des tests de pénétration des applications effectués sur les composants concernés.

OPS-17: Les composants technologiques critiques visés à l'OPS-02 sont régulièrement mis à jour avec, dans la mesure du possible, la dernière version disponible des logiciels associés (tels que le système d'exploitation, l'environnement d'exécution (*runtime*), les micrologicels (*firmware*) et les kits de développement logiciel (*SDK*)). Des exceptions peuvent être faites pour des raisons de stabilité et d'interopérabilité si le risque de sécurité est correctement évalué (notamment en ce qui concerne les correctifs de sécurité).

OPS-18: Tous les processus concernant le traitement des actifs digitaux sont examinés et approuvés par la direction de la partie chargée de la conservation des CP de l'ADR de clients. Toute modification est soumise au processus standard de gestion des changements et doit être revue et approuvée avant d'être mise en œuvre.

3.2.2 Recommendations

OPS-19: Il n'est pas possible d'accéder à des fonctions à privilège élevé sans mesures de sécurité supplémentaires telles que l'authentification multifactorielle ou l'approbation par un quorum. D'autres contrôles de sécurité appropriés peuvent être envisagés pour restreindre l'accès aux fonctions utilisateur. La définition des fonctions à privilège élevé dépend du prestataire de services de conservation et prendre par exemple la forme de privilèges "admin" ou "superadmin".

OPS-20: L'accès aux informations critiques (telles que les données des clients) et aux opérations critiques (telles que la réalisation de transactions) via les API nécessite des autorisations et authentifications explicites, généralement réalisées au moyen de jetons d'authentification spécifiques à chaque compte ou de CP. Ces autorisations sont soumises à des limitations temporelles raisonnables, par exemple par le paramètre de durée de vie d'un jeton ou la date d'expiration d'un certificat.

OPS-21: Les données d'identification requises pour accéder à l'application de gestion de la conservation ou à ses composants ou pour les utiliser (tels que les mots de passe, les codes PIN ou les CP) ne sont pas stockées en clair (c'est-à-dire en texte clair et ne sont pas accessibles sans privilège élevé ou sans authentification supplémentaire) sur les systèmes accédant à l'application. Au lieu de cela, on peut y accéder par des coffres forts digitaux ou des jetons matériels distincts.

OPS-22: Les journaux d'opérations sont protégés de façon à exclure toute modification, ajout ou suppression. Toute tentative d'altération doit être enregistrée. Les journaux ne doivent pas contenir d'informations sensibles telles que des mots de passe ou des CP.

OPS-23: Les contrôles de sécurité critiques sont réalisés dans un environnement d'exécution sécurisé, tel qu'une enclave sécurisée, un système d'exploitation renforcé dédié ou un HSM.

OPS-24: Toutes les opérations peuvent être temporairement suspendues en tout temps par un mécanisme spécifique, par exemple en cas de suspicion d'incident de sécurité.

VOLET D'INFRASTRUCTURE

§ 3.3 Génération de secrets

Cette section traite des aspects de sécurité liés à la génération de secrets cryptographiques, généralement des semences ou des CP appelées ici "clés" par mesure de simplification. Le but principal du fournisseur de services de conservation est de démontrer qu'il dispose d'une assurance adéquate quant au processus de génération des secrets, la confidentialité des valeurs générées tout au long de ce processus et aux mesures prises pour réduire au minimum le risque de perte permanente des secrets.

Les E&R suivantes ne visent pas à couvrir tous les aspects de sécurité d'une procédure de cérémonie des clés, mais se concentrent sur la sécurité des secrets en termes de confidentialité, d'intégrité et de possibilité de récupération.

Le terme "cérémonie des clés" désigne ici la procédure au cours de laquelle les secrets sont générés de façon sécurisée, dans un environnement sûr, sous la supervision de personnes de confiance. L'organisation de la cérémonie des clés peut varier selon les solutions de conservation choisies, mais toute solution doit inévitablement générer des secrets, créer des valeurs de récupération et les stocker sur plusieurs supports et/ou en plusieurs endroits.

En particulier, les systèmes utilisant des signatures multipartites (à seuil) doivent garantir que les secrets (et leurs éléments) sont générés de manière à minimiser le risque d'accès non autorisé et de fuite. Cette génération peut être centralisée ou s'effectuer au moyen d'un protocole de génération de clés distribué.

3.3.1 Exigences

GEN-00: Les secrets sont générés au moyen d'un générateur cryptographique aléatoire ou pseudo-aléatoire dont la logique interne (algorithme, sources d'entropie) est connue et documentée. L'assurance de la sécurité est fournie par des facteurs comprenant au moins l'un des éléments suivants: évaluations externes de la sécurité, conformité à une norme fiable ou autre preuve factuelle que le générateur pseudo-aléatoire est d'un type reconnu ayant résisté à des attaques dans un environnement réel et hostile.

GEN-01: Les sources d'entropie du générateur pseudo-aléatoire sont identifiées et il existe au moins un moyen heuristique de quantifier l'entropie minimale du générateur lors de la création des secrets et de s'assurer qu'elle est suffisante pour générer des clés sûres.

Par exemple, pour générer des CP pour Bitcoin ou Ethereum, qui sont des valeurs scalaires de 256 bits qui doivent être uniformément distribuées, un minimum de 256 bits d'entropie est en théorie nécessaire.

GEN-02: Le protocole de cérémonie des clés est documenté avec suffisamment de précision pour pouvoir être exécuté par des personnes familiarisées avec les actifs digitaux et les outils technologiques connexes et disposant de l'équipement nécessaire.

GEN-03: Les secrets à partir desquels les clés de signature sont dérivées sont générés exclusivement lors d'une cérémonie des clés exécutée conformément à la procédure approuvée.

GEN-04: Les éléments de logiciel critiques utilisés lors d'une cérémonie des clés sont identifiés, leur logique interne est connue et documentée et sont, dans la mesure du possible, utilisés dans leur dernière version stable disponible. Les logiciels critiques peuvent inclure des éléments de logiciel fonctionnant sur une plate-forme intégrée, comme un HSM ou un téléphone portable.

GEN-05: Les éléments de matériel essentiels utilisés pour une cérémonie des clés sont identifiés et le matériel destiné aux cérémonies des clés (ordinateur portable ou imprimante, par exemple) a été spécifiquement acquis à cette fin. La chaîne de conservation du matériel n'a pas été rompue et l'accès est contrôlé de façon ininterrompue par la partie qui organise la cérémonie des clés. Il est à noter que des éléments de matériel (tels que des HSM) peuvent être utilisés en production avant et après une cérémonie des clés.

GEN-06: Lors d'une cérémonie des clés, dès lors qu'un dispositif électronique interagit avec des secrets, il est déconnecté de tout système qui ne participe pas aux opérations de la cérémonie des clés et à l'architecture qui s'y rapporte (comme des périphériques sans fil ou des services en ligne ne jouant aucun rôle dans la cérémonie). Les connexions autorisées peuvent inclure des services accessibles par internet.

GEN-07: Pour les systèmes à signature unique (par opposition aux systèmes à signatures multiples), les secrets et les informations qui s'y rapportent générés lors de la cérémonie des clés ne sont jamais exposés visuellement aux participants à la cérémonie.

Pour permettre différents types de sauvegardes, il est toutefois toléré que les valeurs secrètes liées à une multi-signature ou au partage des secrets à seuil soient visuellement exposées à des parties autorisées, comme par exemple à des conservateurs de clés. Cette tolérance existe pour autant que nul n'obtienne d'accès visuel à des informations se rapportant aux clés allant au-delà de ce qui serait le cas pour un fonctionnement normal du système.

GEN-08: Les copies des clés ou des valeurs sensibles qui s'y rapportent (telles que les partages et les sauvegardes) conservées temporairement sur un appareil (tel qu'un support de stockage externe ou un ordinateur portable) sont effacées de façon sécurisée avant la fin de la cérémonie (sauf pour les supports utilisés à des fins de sauvegarde). Des mesures sont prises pour empêcher l'extraction à partir de la mémoire vive ou d'autres mémoires temporaires du système.

L'effacement sécurisé vise à empêcher une personne ou un programme informatique de reconstruire ces données après la cérémonie, et nécessite généralement des techniques effaçant les données plusieurs fois et les écrasant avec des valeurs sans rapport de façon à empêcher la récupération de la mémoire.

GEN-09: Un rapport est établi à l'issue d'une cérémonie des clés, comprenant au moins l'identité des personnes impliquées, leurs rôles et responsabilités respectifs, la liste des éléments utilisés (logiciels et matériel, avec leur numéro de version), la liste des opérations effectuées, et tout écart par rapport au protocole documenté. Ce document est conservé en lieu sûr pour assurer la traçabilité et permettre la vérification du processus.

3.3.2 Recommendations

GEN-10: Le code source, ou au moins le code binaire, du générateur aléatoire ou pseudo-aléatoire utilisé pour générer des secrets est disponible pour inspection lors des évaluations de sécurité.

GEN-11: Les récepteurs sans fil des appareils électroniques utilisés lors d'une cérémonie des clés sont physiquement désactivés (par exemple, retirés de leur boîtier ou débranchés).

§ 3.4 Récupération de secrets

Des processus de récupération des secrets doivent être mis en place pour reconstituer les secrets générés en cas de perte, de destruction ou d'indisponibilité du support utilisé pour les opérations usuelles. Comme le soulignent les E&R ci-dessous, le mécanisme de récupération des secrets doit être conçu de façon à ce qu'aucune partie ne puisse récupérer un ou plusieurs secrets de façon indépendante, et de manière à réduire le risque de perte permanente.

Dans ce qui suit, un élément de récupération de secret (ou simplement **élément de récupération**) est un élément physique tel qu'un support de stockage, un ordinateur portable ou un morceau de papier servant à stocker des données qui peuvent être utilisées pour reconstituer un ou plusieurs secrets générés lors d'une cérémonie des clés. Ces données sont appelées **valeurs de récupération**.

3.4.1 Exigences

REC-00: Les éléments de récupération sont créés lors de la cérémonie des clés exclusivement. Après la cérémonie des clés, les éléments de récupération ne peuvent être manipulés qu'avec des mesures de protection adéquates en termes de confidentialité et d'intégrité.

REC-01: Des procédures sont définies de façon à ce qu'aucune partie ou système ne puisse récupérer seul les composants et reconstruire ou utiliser les clés générées après la cérémonie. Cela peut par exemple être obtenu par une solution de partage de secrets à seuil et d'une distribution des éléments de secret sur des sites distincts. Dans les cas où aucun partage de secret n'est utilisé et où un élément de récupération unique contient une ou plusieurs clés, des procédures supplémentaires doivent être mises en place pour empêcher qu'une personne seule puisse accéder aux éléments de récupération.

REC-02: La validité de tous les éléments de récupération est vérifiée pendant la cérémonie des clés au cours de laquelle ces derniers sont créés. En particulier, lorsqu'une solution de partage de secret est utilisée, une étape de vérification doit porter sur le fait que toute combinaison valide des éléments partagés produira le secret attendu.

REC-03: Le processus de récupération est documenté et accessible à la partie responsable. Il est régulièrement revu et testé pour vérifier que les secrets peuvent être reconstitués en cas de besoin. Les personnes concernées reçoivent une formation sur la façon de procéder en cas de récupération. La documentation est tenue à jour.

La mise à jour de la documentation peut être cruciale lorsqu'un secret est reconstitué à l'aide d'une version de logiciel plus récente que celle qui avait été utilisée pour générer le secret. L'utilisation de la version plus récente du logiciel peut ne pas être conforme au processus de récupération initialement documenté.

REC-04: Des plans de reprise après sinistre et de continuité des activités ont été établis et documentés pour la solution de conservation, et ces plans couvrent le processus de récupération des secrets.

3.4.2 Recommendations

REC-05: Les éléments de récupération sont stockés sur plusieurs sites physiques distincts du site d'exploitation (c'est-à-dire l'endroit où les secrets sont stockés et utilisés). Ces sites doivent être dotés de systèmes de sécurité adéquats permettant de détecter et d'empêcher les accès non autorisés (physiques et logiques) aux éléments de récupération.

Par sites physiques distincts, il faut entendre des bâtiments ou des villes distincts plutôt que des pièces ou des coffres forts séparés. Dans ce contexte, l'accès logique signifie la capacité d'accéder aux éléments de

récupération par déduction, en utilisant par exemple des informations d'identification telles qu'une phrase-clé, un certificat ou une clé cryptographique.

REC-06: Les valeurs de récupération sont calculées à l'aide d'un modèle de quorum (tel qu'un partage de secret à seuil, ou tout autre mécanisme équivalent en termes d'accès et de distribution de la confidentialité) nécessitant au moins deux parties pour reconstruire le secret.

REC-07: Les valeurs de récupération sont stockées séparément (c'est-à-dire sur des composants de recouvrement différents) pour des secrets différents, de telle sorte que l'accès à un composant de récupération pour un secret n'entraîne pas l'accès à celui d'un autre secret.

Cela signifie qu'un support de stockage spécifique peut être utilisé pour chaque élément d'un secret. Si plusieurs éléments d'un secret sont stockés sur un même support, des éléments d'identification distincts doivent être nécessaires pour accéder à chacun des éléments. Si par exemple dix secrets indépendants sont protégés par cinq éléments de récupération chacun, cinquante unités de support de stockage seraient nécessaires, ce qui pourrait s'avérer peu pratique et source d'erreurs.

REC-08: Les valeurs de récupération sont stockées sur au moins deux types de supports, généralement un composant électronique et un composant non électronique, tels qu'une mémoire flash ou du papier. Cela permet d'atténuer le risque de perte lié à la nature exclusivement physique ou électronique du support.

REC-09: L'intégrité des éléments de récupération est régulièrement vérifiée et l'accès à ces éléments est contrôlé, enregistré et périodiquement vérifié. Des contenants sensibles aux altérations (tels que des sacs de sécurité ou des enveloppes scellées) doivent être utilisés pour s'assurer que les valeurs de récupération n'ont pas été modifiées.

§ 3.5 Développement et maintenance

Cette section traite de questions liées au développement et à la maintenance de la solution de garde, notamment des mesures tendant à minimiser le risque de création de faiblesses de sécurité, que ce soit par accident ou par malveillance. Dans cette perspective, des mesures de prévention et de détection appropriées doivent être mises en place par la distribution des secrets, le maintien d'un niveau de qualité élevé et la garantie d'un niveau de transparence adéquat.

3.5.1 Exigences

DEV-00: L'autorisation de modifier le code source, la configuration, la documentation et d'autres composants critiques de la solution n'est accordé que quand cela est nécessaire; cet octroi est dûment documenté.

Si le code source du prestataire de services de conservation est partiellement ouvert (par exemple dans un dépôt public GitHub), DEV-00 requiert que l'acceptation des modifications apportées ou demandées par des tiers soit soumise à des contrôles spécifiques.

DEV-01: L'accès au code source, à la configuration, à la documentation ou à d'autres composants critiques de la solution à partir d'internet nécessite une authentification à deux facteurs.

DEV-02: Les listes de contrôle d'accès et les autres autorisations sont régulièrement examinées par des personnes responsables et sont adaptées de façon à maintenir le nombre d'autorisations aussi bas que possible, que ce soit pour des personnes ou des services. L'examen des autorisations est documenté de manière adéquate.

DEV-03: Dans la mesure du possible, chaque modification apportée à un composant du système, en particulier à son code source, est consignée de manière à indiquer l'heure de l'opération et la personne responsable. Ceci est typiquement réalisé par des systèmes modernes de contrôle de version tels que *git*.

DEV-04: Les composants tiers à code source ouvert sont identifiés et régulièrement vérifiés pour détecter les erreurs ou vulnérabilités nouvellement identifiées.

DEV-05: Les éléments de logiciel essentiels de la solution et les modifications qui y sont apportées font l'objet d'un examen et de tests internes et/ou externes avant d'être déployés en production. Les examens en question (tels que les examens du code source ou les essais automatisés) sont documentés.

DEV-06: Des évaluations de la sécurité sont effectuées par des tiers au moins une fois par an sur un ou plusieurs composants critiques de la solution de conservation. Les rapports d'évaluation comprennent des descriptions de toute lacune identifiée; des mesures de remédiation sont mises en œuvre et documentées.

DEV-07: Les personnes responsables du développement de la solution (ingénieurs ou membres du management) n'ont pas d'accès permanent aux systèmes de production. Il ne peut être dérogé à cette règle que temporairement, dans des situations d'urgence et de manière dûment autorisée, supervisée, documentée et journalisée.

3.5.2 Recommendations

DEV-08: Les éléments de logiciel critiques, tels que ceux qui interagissent avec des valeurs secrètes ou ceux qui effectuent des contrôles de sécurité, bénéficient d'une assurance de sécurité renforcée (par exemple par le biais d'évaluations de sécurité réalisées par des tiers ou de certifications formelles), en particulier si le code source n'est pas disponible pour inspection par leurs utilisateurs.

DEV-09: L'équipe de développement met en œuvre un cycle documenté et sécurisé de développement de logiciel et emploie au moins une personne responsable de la sécurité. Ce cycle de développement peut inclure des tests de sécurité automatisés et des méthodes de découverte des vulnérabilités.

DEV-10: Les évaluations de sécurité réalisées conformément à DEV-06 comprennent à la fois des audits ciblés des éléments critiques (par exemple, d'un éventuel code cryptographique propriétaire) et des audits de type *Red Team* couvrant l'ensemble de la surface d'attaque de la solution.

ANNEXE A - GLOSSAIRE

Termes	Définitions
Actifs digitaux	Tout types d'actifs financiers, qu'ils soient nativement numériques ou numérisés, émis à l'aide de la TRD, tels que des jetons de paiement (y compris les crypto-monnaies), des jetons d'utilité ou des jetons représentant des instruments financiers ou des valeurs mobilières.
ADR	Adresse de registre distribué (*Distributed Ledger Address / Account* ou *DLA*). Le compte ou l'adresse du registre distribué est un identifiant unique sur un registre distribué particulier, qui sert d'emplacement virtuel pour l'enregistrement de transactions entrantes et sortantes portant sur un ou plusieurs actifs digitaux.
API	*Application programming interface* ou interface de programmation d'application, c'est-à-dire fonctionnalité informatique permettant à deux systèmes de communiquer.
Authentification à deux facteurs	Méthode permettant de confirmer l'identité ou les droits d'accès revendiqués par un utilisateur en utilisant une combinaison de deux facteurs (par exemple, un mot de passe et une confirmation envoyée par l'intermédiaire d'un appareil mobile).
Cérémonie des clés	Procédure par laquelle les secrets sont générés d'une manière qui garantit leur force cryptographique et minimise le risque de fuite ou de sabotage. Une cérémonie des clés comprend généralement d'autres opérations telles que le chargement de composants logiciels dans du matériel de confiance.
CP	Clé privée.
CMTA	Capital Markets and Technology Association.
DACS	*Digital Assets Custody Standard* ou Standard pour la conservation d'actifs digitaux.
Elément de récupération de secret ou Elément de récupération	Information ou une valeur stockée sur un support, ou composant matériel (inviolable) qui peut être utilisé pour reconstruire un secret généré lors d'une cérémonie des clés.
Entropie	Entrées aléatoires collectées par ordinateur. La référence à un processus de "collecte" s'explique par le fait que les ordinateurs ne peuvent pas - à proprement parler - générer d'entrées aléatoires, mais utilisent des données apparemment insignifiantes pour émuler le hasard, par exemple en mesurant le temps écoulé entre les mouvements de la souris ou la température du système. Une CP avec une entropie de X bits signifie que la CP est aussi forte qu'une chaîne de X bits choisis au hasard.
E&R	Exigences et recommandations.
Fonctions d'administration	Capacité technique d'apporter des modifications majeures à un système. On parle aussi parfois de "privilèges administratifs".
Fonctions utilisateur	La capacité technique d'utiliser les fonctions attribuées à des utilisateurs.
HSM	*Hardware security module* ou module matériel de sécurité: un processeur cryptographique sécurisé axé sur la génération de clés cryptographiques et qui réalise des opérations cryptographiques accélérées au moyen de ces clés.

MPC	*Multi-party computation methods* ou méthodes de calcul multipartites tels que des mécanismes à signatures multiples, multipartites, globales ou à seuil.
Partage de secret à seuil	Méthode consistant à diviser un secret en plusieurs éléments et à exiger un nombre minimum déterminé d'éléments pour que le secret soit percé.
Preuve de réserve (*proof-of-reserve*, PoR)	Preuve que le dépositaire détient les actifs qu'il prétend détenir.
Registre distribué	Une base de données qui est partagée et synchronisée de manière consensuelle selon un protocole par des nœuds participant à un réseau décentralisé pair-à-pair. Le registre permet aux transactions d'avoir des "témoins" publics, qui peuvent accéder aux enregistrements partagés sur le réseau et peuvent chacun en stocker une copie identique. Toute modification ou ajout apporté au registre est répercuté et copié auprès de l'ensemble des nœuds. Une forme de registre distribué est la blockchain, qui peut être publique, autorisée ou privée.
Registre interne	Le registre interne est en substance une base de données privée gérée par le dépositaire afin d'attribuer les soldes de chaque ADR contrôlée par le dépositaire à un ou plusieurs clients ou comptes, de sorte que, dans les livres et registres du dépositaire, soit (i) les actifs crédités sur une ADR peuvent être attribués individuellement à un client ou à un compte, soit (ii) lorsque les actifs crédités sur une ADR sont attribués à un groupe de clients ou de comptes (ADR groupées), la part de chaque client ou de chaque compte dans le groupe peut être clairement déterminée.
SDK	*Software Development Kit* en anglais: Kit de développement logiciel.
Semence	Une entrée (généralement sous forme de texte) utilisée pour générer une paire de clés publique / privée.
Signature à seuil	Méthode qui consiste à diviser une clé privée en plusieurs éléments et à exiger qu'un nombre minimum déterminé d'éléments pour qu'une signature conjointe soit délivrée.
Technologie des registres distribués (TRD)	Technologie d'enregistrement et de partage de données entre plusieurs magasins de données (ou registres). Cette technologie permet d'enregistrer, de partager et de synchroniser des transactions et des données sur un réseau distribué composé de différents participants.
TLS	*Transport Layer Security*: protocole cryptographique standard pour les communications sécurisées sur des réseaux informatiques.
Valeur de récupération	Elément physique tel qu'un support de stockage, un ordinateur portable ou un morceau de papier servant à stocker des données qui peuvent être utilisées pour reconstituer un ou plusieurs secrets.

ANNEXE B - VERSIONS DU DACS

Version	Date	Description
V2	Mars 2023	Revue par les parties prenantes de la CMTA et adaptation reflétant certains développements dans le domaine de la conservation d'actifs (en particulier pour ce qui concerne les solutions fondées sur des MPC). Requalification de certaines recommandations en exigences conformément aux discussions intervenues au sein du groupe de travail. Reformulation de certaines exigences pour en faciliter la vérification indépendante. Adaptations formelles et clarifications rédactionnelles diverses.
V1	Octobre 2020	Version originale du DACS.