INSTRUCTION AMF

DOC-2019-24

PRESTATAIRES DE SERVICES SUR ACTIFS NUMERIQUES - REFERENTIEL D'EXIGENCES EN MATIERE DE CYBERSECURITE (VERSION 1.0)

Texte de référence : article 721-4 du règlement général de l'AMF

1. INTRODUCTION

1.1. PRESENTATION GENERALE

1.1.1. Contexte

La loi n°2019-486 du 22 mai 2019 relative à la croissance et à la transformation des entreprises, dite loi PACTE, comprend un article 86 relatif aux prestataires de services sur actifs numériques dont les dispositions sont précisées par décret et par le règlement général de l'AMF.

L'article 721-4 du règlement général de l'AMF fait ainsi référence à la sécurité des systèmes d'information, dénommée également « cybersécurité », pour les demandeurs de l'agrément de prestataire de services sur actifs numériques :

« *Lorsque l'AMF demande au demandeur de recourir à des produits évalués et certifiés ou de faire procéder à des audits de sécurité pour l'application des articles D. 54-10-7 et D. 54-10-9 du code monétaire et financier, l'évaluation des produits et l'audit de sécurité sont réalisés conformément à une instruction relative au référentiel d'exigences*. »

Ces exigences visent à s'assurer que les prestataires de services sur actifs numériques disposent d'un système d'information résilient et sécurisé face aux menaces afférentes à cet écosystème, à savoir entre autres :

- la compromission de portefeuilles détenant des actifs numériques ;
- la fuite de données à caractère personnel ;
- les attaques par déni de service ;
- l'usurpation d'identité ;
- l'incapacité à investiguer en cas d'incident ou d'activité frauduleuse.

1.1.2. Objet du document

Ce document a ainsi pour objectif de détailler les exigences requises par l'AMF dans le cadre de l'article 721-4 du règlement général de l'AMF, pour chaque service sur actifs numériques couverts par la loi PACTE, pour la fourniture duquel un demandeur peut demander l'agrément.

1.1.3. Les services sur actifs numériques

La liste des services sur actifs numériques figure à l'article L. 54-10-2 du code monétaire et financier :

- **1)** le service de conservation pour le compte de tiers d'actifs numériques ou d'accès à des actifs numériques, le cas échéant sous la forme de clés cryptographiques privées, en vue de détenir, stocker et transférer des actifs numériques (« service de conservation ») ;
- **2)** le service d'achat ou de vente d'actifs numériques en monnaie ayant cours légal ;
- **3)** le service d'échange d'actifs numériques contre d'autres actifs numériques ;
- **4)** l'exploitation d'une plateforme de négociation d'actifs numériques ;
- **5a)** la réception et la transmission d'ordres sur actifs numériques pour le compte de tiers ;
- **5b)** la gestion de portefeuille d'actifs numériques pour le compte de tiers ;
- **5c)** le conseil aux souscripteurs d'actifs numériques ;
- **5d)** la prise ferme d'actifs numériques ;
- **5e)** le placement garanti d'actifs numériques ;
- **5f)** le placement non garanti d'actifs numériques.

1.2. ACRONYMES ET DEFINITIONS

1.2.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont les suivants :

ANSSI : Agence nationale de la sécurité des systèmes d'information
CNIL : Commission nationale de l'informatique et des libertés

- **CSPN** : Certification de sécurité de premier niveau
- **DEEP** : Dispositif d'enregistrement électronique partagé
- **PASSI** : Prestataire d'audit de la sécurité des systèmes d'information
  PSAN : Prestataire de services sur actifs numériques
  RGPD : Règlement général sur la protection des données personnelles
- **RGS** : Règlement général de sécurité

1.2.2. Définitions

Un « **demandeur** » désigne une organisation, publique ou privée, souhaitant obtenir l'agrément de l'AMF pour la fourniture d'un ou plusieurs service(s) sur actifs numériques mentionné(s) à l'article L. 54-10-2 du CMF.

Un « **portefeuille électronique** » désigne une solution logicielle ou matérielle de conservation d'actifs numériques, généralement composée de deux clés cryptographiques : l'une publique, permettant la réception d'actifs numériques ; et l'autre privée, permettant la signature d'une transaction d'actifs numériques.

Un portefeuille électronique peut être dit « **en ligne** » (*hot wallet*), c'est-à-dire présent sur un système connecté et visible sur Internet ; ou « **hors ligne** » (*cold wallet*) ainsi non connecté à Internet.

2. EXIGENCES GENERALES APPLICABLES A TOUS LES SERVICES

2.1. LUTTE ANTI-BLANCHIMENT ET FINANCEMENT DU TERRORISME

Le demandeur doit tracer et conserver les traces de toute activité engendrée par le service sur actifs numériques offert, pendant une durée de 5 ans, au moyen d'un dispositif permettant d'en assurer la disponibilité, la confidentialité, l'intégrité et la non-répudiation. Les accès à ce dispositif et les traces associées doivent également répondre à cette même exigence.

Les dispositifs impliqués doivent respecter les bonnes pratiques de l'ANSSI en matière de journalisation des traces [JRNANSSI].

2.2. RESPONSABILITES LIEES A LA SOUS-TRAITANCE

Le prestataire de services sur actifs numériques est, vis-a-vis de l'AMF, pleinement responsable de la cybersécurité du service sur actifs numériques pour la fourniture duquel il détient un agrément.

3. EXIGENCES GENERALES APPLICABLES A TOUS LES SERVICES EXCEPTE LE SERVICE DE CONSEIL AUX SOUSCRIPTEURS D'ACTIFS NUMERIQUES

3.1. PROGRAMME DE CYBERSECURITE

Le demandeur doit définir, formaliser, mettre en œuvre et contrôler un programme continu de cybersécurité visant à maitriser le niveau de sécurité des systèmes d'information impliqués dans la fourniture du ou des services sur actifs numériques. Ce programme doit notamment comprendre :

1°) dès la phase de conception, l'analyse des risques de sécurité qui pourraient impacter négativement la disponibilité, l'intégrité, la confidentialité et la traçabilité (DICT) des systèmes

d'informations. Cette analyse doit permettre d'identifier et d'évaluer la probabilité et l'impact de ces risques, ainsi que l'identification des mesures de sécurité permettant de les maitriser. Les systèmes d'information critiques, les services de sécurité et les données sensibles évaluées en rapport aux critères DICT doivent être spécifiquement listés et les intervenants sur ceux-ci doivent être spécifiquement sensibilisés ;

2°) l'analyse d'impact relative à la protection des données à caractère personnel (AIPD). Cette analyse doit permettre d'évaluer le niveau de risque engendré par le traitement pour les droits et libertés des personnes physiques et prevoir les mesures appropriées pour atténuer ce risque. Le demandeur doit en outre s'assurer de la conformité de ses traitements avec le règlement n° 2016/679, dit règlement général sur la protection des données (RGPD), en particulier sur le respect des obligations liées à la sous-traitance ou les règles encadrant les transferts internationaux de données personnelles ;

3°) la mise en œuvre de moyens humains, organisationnels et techniques permettant de maitriser les risques identifiés et de répondre aux exigences de disponibilité, intégrité, confidentialité et traçabilité définies ;

4°) les dispositifs de contrôle de la présence et de l'efficacité des mesures de sécurité préalablement identifiées ;

5°) les procédures de revue régulière des comptes et des droits d'accès sur les systèmes d'information listés précédemment ;

6°) la gestion des vulnérabilités incluant une veille sur les vulnérabilités techniques et menaces pouvant apparaître ainsi que l'application d'une politique permettant leur traitement ;

7°) les moyens humains et techniques permettant la détection d'intrusion ou plus généralement d'évènements redoutés sur les systèmes d'information listés précédemment ;

8°) les procédures de réponse face aux incidents de sécurité et la reprise de l'activité nominale.

A cette fin, les guides suivants peuvent constituer des référentiels :

a. le guide d'hygiène informatique de l'ANSSI [HYGANSSI] ;
b. le guide de la sécurité des données personnelles de la CNIL [SECCNIL] ;
c. les premiers éléments d'analyse de la CNIL au regard de la technologie Blockchain [BLCNIL].

Par ailleurs, EBIOS Risk Manager [EBIOS] peut constituer une méthode pour l'analyse des risques.

Les politiques internes du demandeur relatives aux thèmes et chapitres de la norme ISO 27002 doivent être formalisées, vérifiées et contrôlées. Elles doivent être revues et adaptées, si nécessaire, au moins une fois par an, ou en cas de survenance d'un événement le justifiant. Il n'est néanmoins pas exigé du demandeur de disposer d'une certification ISO 27001.

Le demandeur doit désigner un responsable de la sécurité des systèmes d'information, en charge de décliner le programme de cybersécurité, et communiquer ses coordonnées à l'AMF.

3.2. MESURES OPERATIONNELLES

Partant du constat qu'à date, la quasi-intégralité des services sur actifs numériques sont offerts via un site Web ou une application mobile, cette section a pour objectif de lister des exigences techniques générales permettant d'en assurer un niveau de sécurité minimum.

3.2.1. Sécurité des composants

Les composants techniques impliqués dans la fourniture du service doivent être identifiés et maintenus à jour.

De plus, la liste des dépendances doit être maîtrisée afin de s'assurer de la confiance dans les composants déployés pour la fourniture du service.

Les configurations des composants techniques impliqués dans la fourniture du service doivent être durcies conformément aux analyses de risques effectuées. Les sources suivantes peuvent constituer des référentiels pour cette exigence :

a. les guides de configuration et bonnes pratiques de l'ANSSI [BPANSSI] ;
b. les guides de configuration de l'association Center for Internet Security [CIS].

3.2.2. Sécurité des développements applicatifs

Les développements applicatifs effectués par le demandeur pour offrir son service sur actifs numériques doivent prendre en compte les référentiels de sécurité applicative suivants :

a. le Top 10 des recommandations générales de l'OWASP [OWASPR] ;
b. le Top 10 courant de l'OWASP pour la sécurité des applications Web [OWASPW] ;
c. le Top 10 Mobile courant de l'OWASP pour la sécurité des applications mobiles [OWASPM].

3.2.3. Authentification

3.2.3.1. Des noms de domaine

Les noms de domaine utilisés pour la fourniture du service sur actifs numériques doivent être authentifiés par l'extension DNSSEC [DNSSEC].

3.2.3.2. Des services techniques exposés sur Internet

Le demandeur doit authentifier les services qu'il expose sur Internet au moyen d'un certificat X.509 signé par une Autorité de Certification reconnue publiquement.

Le demandeur, lorsqu'il propose une application mobile, doit mettre en œuvre une mesure d'épinglement de certificat afin d'authentifier fortement le service technique distant [PIN].

3.2.3.3. Des utilisateurs

Le demandeur doit permettre, par défaut, aux utilisateurs de son service de pouvoir s'authentifier avec un second facteur en plus du mot de passe habituel. Un message clair informant des risques associés à l'absence de double facteur doit être affiché à l'utilisateur et son consentement explicite doit être obtenu pour ne pas bénéficier de cette protection.

3.2.3.4. Des administrateurs

Le demandeur doit authentifier fortement au moyen d'un mécanisme à double facteurs les administrateurs techniques et fonctionnels sur le ou les systèmes d'information.

3.2.4. Chiffrement

3.2.4.1. Des communications

Les flux de communications impliqués dans la fourniture du service et son administration doivent être systématiquement chiffrés au moyen de protocoles et algorithmes de chiffrement robustes conformes au référentiels suivant en matière de choix des protocoles et algorithmes à supporter : l'annexe B1 du RGS [RGSB1].
Plutôt que de développer ses propres solutions, le demandeur est très fortement encouragé à recourir à des implémentations éprouvées et disposant d'un suivi de sécurité.

3.2.4.2. Des données

Le demandeur doit garantir à l'utilisateur une protection en confidentialité et en intégrité de ses données. Cette garantie ne doit pas reposer sur la seule protection périmétrique du service offert, et doit couvrir plus globalement le risque d'intrusion dans le service par un attaquant.

3.3. SECURITE DES PORTEFEUILLES ELECTRONIQUES

Le demandeur doit conseiller à ses utilisateurs l'usage de portefeuilles électroniques disposant d'un niveau de sécurité conforme à l'état de l'art, mettant par exemple en œuvre :

a. une protection par mot de passe ou clé de chiffrement ; et/ou

b. un chiffrement des secrets, dont notamment la clé privée, conformément aux recommandations techniques de l'annexe B1 du RGS [RGSB1] ; et/ou

c. une conservation hors-ligne.

3.4. SECURITE DU DEEP

Dans le cas d'utilisation d'un DEEP spécifiquement conçu par le demandeur même ou un de ses fournisseurs pour les besoins du service requis, l'AMF pourra exiger que le DEEP fasse l'objet d'une certification de sécurité dans un schéma reconnu (comme par exemple une Certification de Sécurité de Premier Niveau [CSPN] ou une Certification Critères Communs [CCC]). Cette éventualité sera d'autant plus considérée que le DEEP sera privé, ou issu d'une technologie propriétaire ou dont le code n'est pas disponible en source ouverte (*open-source*).

3.5. AUDIT DE SECURITE

Lorsque l'AMF requiert un audit de sécurité, l'audit doit être réalisé selon les conditions suivantes :

1°) sur le périmètre du système d'information, interne ou externe, impliqué dans la fourniture du ou des services sur actifs numériques pour lequel le prestataire de services sur actifs numériques détient un agrément de l'AMF ;

2°) par un ou plusieurs tiers disposant de la qualification PASSI prévue par l'ANSSI, pour couvrir *a minima* les portées suivantes [PASSI] :

a) audit organisationnel et physique ;

b) audit d'architecture ;

c) audit de configuration ;

d) tests d'intrusion.

Ce ou ces audits doivent être réalisés dans le cadre et les conditions de la qualification PASSI.

Le demandeur doit joindre au rapport d'audit, un document formalisé par son responsable de la sécurité des systèmes d'information, et présenté aux instances dirigeantes du demandeur, explicitant le plan d'actions prévu afin de remédier aux risques et constats identifiés au sein du rapport d'audit.

Le ou les documents constituant le rapport d'audit réalisé par l'auditeur tiers doivent :

a. respecter les exigences de formalisation du chapitre VI.6 du référentiel PASSI [PASSIR] ;

b. intégrer une approche par les risques, notamment en représentant les risques sous une forme matricielle ;

c. être signé électroniquement par le tiers.

3.6. NOTIFICATION D'INCIDENT DE SECURITE

Suite à la survenance d'un incident de sécurité significatif impliquant un service sur actifs numériques, le demandeur doit informer sans délai l'AMF en formalisant une note synthétisant :

a. la nature de l'incident ;
b. le périmètre affecté ;
c. le ou les services sur actifs numériques impactés ;
d. l'impact de l'incident, sur les systèmes et pour les utilisateurs du service ;
e. la méthode et chronologie de détection ;
f. le résultat des investigations menées ;
g. le plan d'action prévu pour remédier à l'incident ;
h. les mesures prises pour éviter qu'un incident similaire se reproduise à l'avenir ;
i. toute autre information pertinente en lien avec l'incident.

4. EXIGENCES SPECIFIQUES APPLICABLES AU SERVICE DE CONSERVATION (1)

L'objectif premier de ce service est de tenir les positions des clients de façon consolidée, par exemple dans un contexte d'utilisation de plusieurs types d'actifs ou plusieurs DEEP.

Pour ce faire, le demandeur peut mouvementer les actifs numériques selon deux cas d'usage :

1) Il possède la capacité de mouvementer les actifs numériques d'un tiers, par exemple en opérant un portefeuille électronique dédié au tiers ou un portefeuille électronique dans lequel figurent les actifs numériques d'un tiers parmi d'autres actifs numériques ;

2) Il conserve les clés cryptographiques privées d'un tiers, c'est-à-dire son portefeuille électronique.

4.1. EXIGENCES COMMUNES AUX DEUX CAS D'USAGE

Les procédures de génération, stockage, sauvegarde, réponse en cas de compromission de clé ou de secret ayant servi à générer les clés (graine ou *seed*), restitution et destruction des portefeuilles électroniques doivent être formalisées, vérifiées et régulièrement contrôlées.

Un stockage hors-ligne des portefeuilles devrait être privilégiée afin de limiter le risque de compromission.

4.2. CONSERVATION D'ACTIFS POUR LE COMPTE DE TIERS

Génération du portefeuille

Un portefeuille unique par utilisateur du service doit être créé.

Dans le cas d'une génération d'un portefeuille de type « déterministe hiérarchique » (*hierarchical deterministic wallet*), la graine et la clé privée doivent être sauvegardées de manière sécurisée avec des moyens appropriés et leur accès doit être contrôlé et tracé.

La caractéristique de multi-signature doit être privilégiée pour la création d'un portefeuille, nécessitant ainsi un quorum (utilisateur, demandeur, etc.) pour signer une transaction.

4.3. CONSERVATION DE CLES PRIVES POUR LE COMPTE DE TIERS

Hormis le portefeuille d'un utilisateur du service, la conservation de tout autre moyen d'accès à des actifs numériques est proscrite, par exemple les authentifiants à un service tiers permettant d'accéder au portefeuille (login et mot de passe, etc.).

5. EXIGENCES SPECIFIQUES APPLICABLES AUX SERVICES D'ACHAT OU DE VENTE D'ACTIFS NUMERIQUES CONTRE D'AUTRES ACTIFS NUMERIQUES EN MONNAIE AYANT COURS LEGAL (2), D'ECHANGE D'ACTIFS NUMERIQUES CONTRE D'AUTRES ACTIFS NUMERIQUES (3), D'EXPLOITATION D'UNE PLATEFORME DE NEGOCIATION D'ACTIFS NUMERIQUES (4) ET DE RECEPTION ET TRANSMISSION D'ORDRES SUR ACTIFS NUMERIQUES POUR LE COMPTE DE TIERS (5a)

NON CONSERVATION D'ACTIFS NUMERIQUES ET DES MOYENS D'ACCES

Le demandeur ne doit pas conserver, pour l'utilisateur du service, d'actifs numériques ou d'accès à des actifs lui appartenant :

a. seule la clé publique de l'utilisateur peut être stockée sur la plateforme offrant le service ;

b. l'utilisateur doit ainsi disposer en propre d'une solution de portefeuille électronique permettant l'envoi ou la réception de l'actif numérique acheté ou vendu.

Si le demandeur exige, pour offrir son service, qu'un utilisateur transfère des actifs numériques sur un portefeuille de dépôt (*deposit wallet*) maitrisé par le demandeur, alors de fait le demandeur conserve des actifs appartenant à l'utilisateur et doit ainsi se conformer aux exigences de sécurité spécifiques applicables au service de conservation (1) définies en paragraphe 4.

6. EXIGENCES SPECIFIQUES APPLICABLES AU SERVICE DE GESTION DE PORTEFEUILLE D'ACTIFS NUMERIQUES POUR LE COMPTE DE TIERS (5b)

UTILISATION DE PORTEFEUILLE DEDIE A LA GESTION DES ACTIFS DE L'UTILISATEUR PAR LE MANDATAIRE

Le demandeur effectuant une activité de gestion de portefeuille d'actifs numériques doit, pour chaque utilisateur de son service (dénommé « mandant » ci-après), créér un portefeuille électronique :

a. dont la clé privée est générée par le mandataire et n'est pas transmise ni connue par le mandant ;

b. opérée par le mandataire avec une solution de portefeuille électronique conforme aux exigences des chapitres 3.3 et 4.2.

Lors de la résiliation du contrat de gestion, le mandataire ne doit pas communiquer au mandant la clé privée du portefeuille électronique utilisé durant le contrat, mais restitue les actifs au mandant via un service de transfert approprié.

Ces dispositions ont pour objectif de garantir la stricte imputabilité des actes de gestion réalisés par le mandataire sur le ou les portefeuilles électroniques du mandant, durant et après résiliation du contrat de gestion.

Si le demandeur opère toutefois les actes de gestion directement sur le portefeuille personnel du mandant, en utilisant la clé privée du mandant, il doit ainsi :

a. se conformer aux exigences de sécurité spécifiques applicables au service de conservation (1) définies en paragraphe 4 ;

b. prendre des dispositions contractuelles spécifiques avec le mandant pour définir le partage des responsabilités en matière d'utilisation frauduleuse des moyens d'accès aux actifs numériques par l'une des parties.

Annexe : Références documentaires

Renvoi	Document
[BLCNIL]	https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-de-donnees-personnelles
[BPANSSI]	https://www.ssi.gouv.fr/administration/bonnes-pratiques/
[CIS]	https://www.cisecurity.org/cis-benchmarks/
[CNIL]	https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
[CSPN]	https://www.ssi.gouv.fr/administration/produits-certifies/cspn/
[DNSSEC]	https://www.ssi.gouv.fr/administration/guide/bonnes-pratiques-pour-lacquisition-et-lexploitation-de-noms-de-domaine/
[EBIOS]	https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/
[HYGANSSI]	https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
[JRNANSSI]	https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/
[OWASPW]	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[OWASPM]	https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
[OWASPR]	https://www.owasp.org/index.php/OWASP_Proactive_Controls
[PASSI]	https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-daudit-de-la-securite-des-systemes-dinformation-passi-qualifies/
[PASSIR]	https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_C.pdf
[PIN]	https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning
[RGSB1]	https://www.ssi.gouv.fr/guide/cryptographie-les-regles-du-rgs/