INSTRUCTION AMF

DOC-2019-24

PRESTATAIRES DE SERVICES SUR ACTIFS NUMERIQUES - REFERENTIEL D'EXIGENCES EN MATIERE DE CYBERSECURITE

Texte de référence : articles D. 54-10-2 et D. 54-10-6 du code monétaire et financier, 721-1-2, 721-1-3 et 721-4 du RGAMF

1. INTRODUCTION

1.1. Présentation générale

1.1.1. Contexte

En application de l'article L. 54-10-3 du code monétaire et financier (« CMF »), avant d'exercer leur activité, les prestataires des services mentionnés aux 1° à 4° de l'article L. 54-10-2 du CMF établis ou fournissant ces services en France sont enregistrés par l'AMF qui vérifie, lorsque ceux-ci sont soumis aux dispositions de l'article L. 54-10-3 du code monétaire et financier en vigueur à compter du 1er janvier 2024 (soumis à l'« enregistrement renforcé »), qu'ils se conforment aux exigences prévues aux 1° à 6° de l'article L. 54-10-3 du CMF.

En application de l'article L. 54-10-5 du CMF, les prestataires établis en France peuvent également solliciter un agrément auprès de l'AMF pour la fourniture à titre de profession habituelle d'un ou plusieurs services mentionnés à l'article L. 54-10-2 du CMF.

Pour obtenir l'enregistrement renforcé et l'agrément, les articles D. 54-10-2 et D. 54-10-6 du CMF renvoient au règlement général de l'AMF (« RGAMF ») pour la liste des documents et informations à communiquer.

L'article 721-4 du RGAMF fait ainsi référence à la sécurité des systèmes d'information, dénommée également « cybersécurité ».

Ces exigences visent à s'assurer que le demandeur dispose 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 sensibles dans le contexte des activités du demandeur et/ou 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.

Ces exigences ne sont pas applicables aux prestataires ayant fait l'objet d'un enregistrement soumis aux dispositions de l'article L. 54-10-3 en vigueur jusqu'au 1er janvier 2024 (soumis à l' « enregistrement simple »).

1.1.2. Objet du document

Ce document a pour objectif de détailler les exigences de l'AMF en application des articles 721-1-2 et 721-4 du RGAMF, pour chaque service sur actifs numériques pour la fourniture duquel le demandeur sollicite un enregistrement renforcé ou un agrément. Le dossier à remettre à l'AMF, dont le contenu est précisé dans le point 7 de cette instruction, comporte une description détaillée de la cybersécurité du demandeur répondant aux éléments énoncés ci-après.

1.2. Acronymes et définitions

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

Le ou les services sur actifs numériques pour lesquels le demandeur sollicite un enregistrement renforcé ou un agrément sont définis à l'article D. 54-10-1 du CMF.

Un « **demandeur** » désigne une organisation, publique ou privée, souhaitant obtenir un enregistrement renforcé ou un 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. Conservation et traçabilité des services fournis

En application de l'article L. 561-12 du CMF relatif aux obligations liées à la lutte contre le blanchiment des capitaux et le 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. La traçabilité et la conservation de ces informations sont également nécessaires dans le cadre de la fourniture des services agréés.

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

2.2. Responsabilités liées à la sous-traitance

Le prestataire de services sur actifs numériques enregistrée de façon renforcée ou agréé demeure en tout état de cause pleinement responsable de la cybersécurité du service sur actifs numériques pour la fourniture duquel il détient un enregistrement renforcé ou un agrément, même lorsqu'il confie à un tiers la définition, la mise en œuvre et/ou le contrôle d'une partie de son dispositif. A ce titre, les dispositifs de contrôle du prestataire, tels que décrits au point 3.1.4 ci-dessous, doivent inclure les prestations ou tâches ainsi confiées audit tiers.

Les relations avec son sous-traitant ou prestataire relatives au système d'information du demandeur sont encadrées par un contrat dont le contenu est précisé dans la position-recommandation AMF DOC-2020-07

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

3.1. Programme de cybersécurité

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 :

1. comprendre a minima les éléments de la présente section 3.1 ;
2. être constitué sous la forme de politiques de sécurité internes au demandeur et validées par les instances dirigeantes, en se basant sur les thèmes et chapitres de la norme ISO 27002.
   Ces politiques 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 avec un rattachement hiérarchique à un niveau suffisamment élevé, et communiquer ses coordonnées à l'AMF.

3.1.1. Analyse de risques d'origine cyber

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'information.
Cette analyse doit permettre d'identifier et d'évaluer la probabilité et l'impact de risques nets et résiduels, ainsi que l'identification des mesures de sécurité permettant de les maitriser et fournir une représentation des risques sous une forme matricielle, sur deux axes orthogonaux, représentant les axes de probabilité et d'impact.
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.

Les scénarios opérationnels impliquant des menaces physiques sur les personnes disposant de privilèges fonctionnels ou techniques, sur les composants permettant l'accès aux actifs numériques ou à de la monnaie ayant cours légal, sont pris en compte dans l'analyse de risques.

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

3.1.2. 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 prévoir 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.

3.1.3. Mesures de prévention

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.

Les guides suivants peuvent constituer des référentiels :

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

3.1.4. Dispositifs de contrôle

Les dispositifs de contrôle de la présence et de l'efficacité des mesures de sécurité préalablement identifiées.
Ces dispositifs de contrôle doivent être constitués par différentes lignes de défense indépendantes entre elles, des équipes opérationnelles jusqu'à l'équipe d'inspection/audit interne. Ces dispositifs de contrôle sont constitués par trois lignes de défense indépendantes entre elles, à savoir : (i) des équipes opérationnelles ; (ii) de l'équipe en charge de la conformité et des risques ; et de l'équipe d'inspection/audit interne.

3.1.5. Revue des comptes utilisateurs et droits associés

Les politiques et procédures de revue régulière des comptes et des droits d'accès sur les systèmes d'information listés précédemment.

3.1.6. Gestion des vulnérabilités

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 selon des engagements temporels adaptés à la criticité des vulnérabilités identifiées.

3.1.7. Mesures de détection

Les moyens humains et techniques permettant la détection d'intrusion ou plus généralement d'évènements redoutés sur les systèmes d'information listés précédemment.

3.1.8. Mesures de réaction

Les politiques et procédures de réponse face aux incidents de sécurité et la reprise de l'activité nominale, incluant le volet de gestion de crise [CRISEANSSI].

3.2. Mesures opérationnelles

Partant du constat qu'à date, la quasi-intégralité des services sur actifs numériques sont offerts via un site Web et/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 guide de bonnes pratiques de l'ANSSI en matière de sécurité des standards du Web [WEBANSSI] ;
b) le Top 10 des recommandations générales de l'OWASP [OWASPR] ;
c) le Top 10 courant de l'OWASP pour la sécurité des applications Web [OWASPW] ;
d) 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 offre un service via 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 robuste [PWANSSI] 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 facteur les administrateurs techniques et fonctionnels sur le ou les systèmes d'information [PWANSSI].

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**x** référentiels suivant**s** en matière de choix des protocoles et algorithmes à supporter : l'annexe B1 du RGS [RGSB1] et le guide ANSSI relatif au chiffrement de flux via le protocole TLS [TLSANSSI]. 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 dans une logique de défense en profondeur.

3.3. Sécurité des portefeuilles électroniques

Le demandeur doit conseiller par écrit à ses clients 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. Sécurité 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 a minima 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. Notification d'incident de sécurité

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 date de survenance de l'incident ainsi que la chronologie des événements ;
b) la nature de l'incident ;
c) le périmètre affecté ;
d) le ou les services sur actifs numériques impactés ;
e) l'impact de l'incident, sur les systèmes et pour les utilisateurs du service ;
f) la méthode et chronologie de détection ;

g) le résultat des investigations menées ;
h) le plan d'action prévu pour remédier à l'incident ;
i) les mesures prises pour éviter qu'un incident similaire se reproduise à l'avenir ;
j) toute autre information pertinente en lien avec l'incident.

4. EXIGENCES SPECIFIQUES APPLICABLES AU SERVICE DE CONSERVATION D'ACTIFS NUMERIQUES POUR LE COMPTE DE TIERS

Dans le cadre de ce service, le demandeur peut mouvementer les actifs numériques, notamment selon deux cas d'usage :

a) Il génère et opère un portefeuille électronique dédié au client, ou un portefeuille électronique dans lequel figurent les actifs numériques du client parmi d'autres actifs numériques ; ou

b) Il détient des moyens d'accès, confiés par le client, lui permettant de mouvementer les actifs numériques du client (par exemple, une clé API).

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 privilégié afin de limiter le risque de compromission.

4.2 Génération du portefeuille

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 des moyens d'accès pour le compte de tiers

La conservation des authentifiants du compte utilisateur du client à un service tiers permettant d'accéder ~~au~~ à ses actifs numériques (login et mot de passe, code temporaire de double authentification etc.) est proscrite.

5. EXIGENCES APPLICABLES POUR LES SERVICES D'ACHAT OU DE VENTE D'ACTIFS NUMERIQUES EN MONNAIE AYANT COURS LEGAL, D'ECHANGE D'ACTIFS NUMERIQUES CONTRE D'AUTRES ACTIFS NUMERIQUES, D'EXPLOITATION D'UNE PLATEFORME DE NEGOCIATION D'ACTIFS NUMERIQUES ET DE RECEPTION ET TRANSMISSION D'ORDRES SUR ACTIFS NUMERIQUES POUR LE COMPTE DE TIERS

Lorsqu'il souhaite être obtenir un enregistrement renforcé ou agréé, pour le service ou les services d'achat ou de vente d'actifs numériques en monnaie ayant cours légal, d'échange d'actifs numériques contre d'autres actifs numériques, d'exploitation d'une plateforme de négociation d'actifs numériques et/ou de réception et transmission d'ordres sur actifs numériques pour le compte de tiers, sans fournir un service de conservation d'actifs numériques pour le compte de tiers, le demandeur ne doit pas conserver des actifs numériques ou des moyens d'accès aux actifs numériques appartenant au client :

a) seule la clé publique du client peut être stockée sur la plateforme offrant le service ;

b) le client 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 client 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 d'actifs numériques pour le compte de tiers, définies en paragraphe 4.

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

Le demandeur souhaitant être agréé pour fournir un service de gestion de portefeuille d'actifs numériques pour le compte de tiers (dénommé « mandataire » ci-après) doit, pour chaque client de son service (dénommé « mandant » ci-après), créer un portefeuille électronique dédié à la gestion des actifs numériques du client :

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

b) opéré 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 d'actifs numériques du mandant il doit :

a) se conformer aux exigences de sécurité spécifiques applicables au service de conservation d'actifs numériques pour le compte de tiers, 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.

7. CONTENU DU DOSSIER DE DEMANDE D'AGREMENT OU D'ENREGISTREMENT

Le dossier à remettre à l'AMF comporte les éléments suivants :

1) le formulaire d'auto-évaluation de conformité au référentiel d'exigences de cybersécurité décrites dans cette instruction ;
2) une analyse du risque d'origine cyber, conformément aux exigences mentionnées au paragraphe 3.1.1 de cette instruction ;
3) le document de cartographie des ressources informatiques listant les ressources informatiques utilisées, le dispositif organisationnel associé, leur criticité pour le demandeur, les interactions entre ressources, et le dispositif de contrôle du risque d'origine cyber sur ces ressources ;
4) un rapport d'audit réalisé par un ou plusieurs tiers disposant de la qualification PASSI prévue par l'ANSSI couvrant les portées suivantes [PASSI] :
    a) audit organisationnel et physique
    b) audit de configuration
    c) test d'intrusion a minima en boites noire et grise
    d) revue de code, dans le cas où le demandeur utilise ou développe des *smart contracts*

Les audits doivent être réalisés dans le cadre et les conditions de la qualification PASSI.

Ils doivent porter sur le périmètre du système d'information, interne ou externe, impliqué dans la fourniture du ou des services sur actifs numériques pour lequel ou lesquels est faite la demande d'agrément ou d'enregistrement renforcé.

L'auditeur PASSI doit contribuer, auprès du demandeur, à la définition du périmètre à auditer en :

- s'appuyant sur les documents 2) et 3)
- recensant les systèmes qu'il évalue, en tant que professionnel de la cybersécurité, comme critiques ou importants en matière des besoins de sécurité (DICT), et au regard des risques intrinsèques de l'activité métier prévue par le demandeur. Par exemple, la conservation d'actifs numériques est un service critique par nature.

- intégrant également les systèmes supportant les processus transverses du demandeur, qui sont souvent ciblés par les attaquants pour ensuite rebondir sur les systèmes métier : messagerie, annuaire, postes de travail, terminaux mobiles etc.

Le demandeur doit joindre au rapport d'audit, un document formalisé par son responsable de la sécurité des systèmes d'information, validé par les instances dirigeantes du demandeur, explicitant le plan d'actions prévu accompagné d'un calendrier de mise en œuvre 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, sur deux axes orthogonaux, l'évaluation des critères de probabilité et d'impact pour les risques identifiés ;

c) être signé électroniquement par l'auditeur tiers.

Lorsque l'AMF demande au demandeur de recourir à des produits évalués et certifiés, le demandeur doit fournir à l'AMF le certificat délivré dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002, conformément à l'article 721-4 du RGAMF.

L'AMF pourra demander des éléments complémentaires en cours d'instruction (politiques, procédures, plans de contrôle, etc.).

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
[SECCNIL]	https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
[CRISEANSSI]	https://www.ssi.gouv.fr/administration/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/
[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://owasp.org/www-project-top-ten/
[OWASPM]	https://owasp.org/www-project-mobile-app-security/
[OWASPR]	https://owasp.org/www-project-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/2014/12/PASSI_referentiel-exigences_v2.1.pdf
[PIN]	https://owasp.org/www-community/controls/Certificate_and_Public_Key_Pinning
[PWANSSI]	https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
[TLSANSSI]	https://www.ssi.gouv.fr/administration/guide/recommandations-de-securite-relatives-a-tls/
[RGSB1]	https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/
[WEBANSSI]	https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-des-sites-web/