AMF INSTRUCTION

DOC-2019-24

DIGITAL ASSETS SERVICE PROVIDERS – CYBERSECURITY SYSTEM OF REQUIREMENTS

Background regulation: Articles D. 54-10-2 and D. 54-10-6 of the French Monetary and Financial Code and 721-1-2, 721-1-3 and 721-4 of the AMF General Regulation

1. INTRODUCTION

1.1. OVERVIEW

1.1.1. Background

Pursuant to Article L. 54-10-3 of the French Monetary and Financial Code ("MFC"), before conducting their activities, services providers mentioned in 1° to 4° of Article L. 54-10-2 of the MFC established or providing services in France are registered with the AMF, which verifies that, when they are subject to the provisions of Article L. 54-10-3 of the MFC in force from January 1, 2024 (subject to "reinforced registration") they comply with the requirements set out in 1° to 6° of Article L. 54-10-3 of the MFC.

Pursuant to Article L. 54-10-5 of the MFC, services providers established in France may also, in order to provide, as their usual profession, one or more services mentioned in Article L. 54-10-2 of the same code, apply to the AMF for a license.

In order to obtain the reinforced registration and the license, Articles D. 54-10-2 and D. 54-10-6 of the MFC refers to the AMF General Regulation for the list of documents and information to provide.

Article 721-4 of the AMF General Regulation refers to the security of information systems, also known as "cybersecurity".
These requirements aim to ensure that the applicant has a resilient and secure information system to manage threats to this ecosystem, including:

- wallets holding digital assets being compromised;
- sensitive data breaches in the context of the applicant's activities and/or a personal context;
- denial of service attacks;
- identity theft;
- inability to investigate in the event of an incident or fraudulent activity.

These requirements do not apply to service providers that have been registered under Article L. 54-10-3 in force until January 1, 2024 (subject to "simple registration").

1.1.2. Document purpose

The purpose of this document is to detail the requirements of the AMF under Articles 721-1-2 and 721-4 of the AMF General Regulation for each digital assets service, for which the applicant may request a reinforced registration or a license. The request to be submitted to the AMF, the content of which is specified in point 7 of this Instruction, includes a detailed description of the applicant's cybersecurity that comply with the following requirements.

1.2. ACRONYMS AND DEFINITIONS

1.2.1. Acronyms

The following acronyms are used in this document:

- **ANSSI**: French National Agency for Information Systems Security
- **CNIL**: French Data Protection Committee (Commission Nationale Informatique et Libertés)
- **CSPN**: First level security certification (certification de sécurité de premier niveau)
- **DLT**: Distributed Ledger Technology
- **PASSI**: Information systems security audit providers' qualification
- **DASPs**: Digital Assets Service Providers
- **GDPR**: General Data Protection Regulation
- **GSR**: General Security Regulation

1.2.2. Definitions

The digital assets service(s) for which the applicant is seeking a reinforced registration or a license is/are defined in Article D. 54-10-1 of the MFC.

An **applicant** refers to an organization, whether public or private, seeking to obtain AMF a reinforce registration or a license for one or many digital assets service(s) referred to in Article L. 54-10-2 of the MFC.

An **electronic wallet** refers to a software or hardware solution for digital assets custody, generally consisting of two cryptographic keys: one public, allowing the reception of digital assets; and the other private, allowing a digital assets transaction to be signed.
An electronic wallet can be said to be **online** (a hot wallet), which is located on a connected system and accessible via the internet; or **offline** (a cold wallet), which is not connected to the internet.

2. GENERAL REQUIREMENTS APPLICABLE TO ALL SERVICES

2.1. CUSTODY AND TRACKING OF SERVICES PROVIDED

Pursuant to Article L. 561-12 of the MFC that states the obligations related to the fight against money laundering and counter terrorist financing, the applicant must track and keep records of all activities generated by the digital assets service provided, for a period of 5 years, using a system to ensure its availability, confidentiality, integrity and non-repudiation. Access to this system and the associated tracking data must also meet the same

requirement. The tracking and custody of these information are also required for the provision of registered services.

The systems involved must comply with the ANSSI best practices for logging tracking data (see JRNANSSI).

2.2. RESPONSIBILITIES RELATED TO SUBCONTRACTING

The reinforced registered or the licensed digital assets services provider remains, in any event, fully accountable for the cybersecurity of the digital assets service for which it is registered as reinforced or licensed even if it entrusts a third party with the definition, implementation and/or control of part of its system. As such, the service provider's control systems, as described in point 3.1.4 below, must include the services or tasks thus services or tasks entrusted to the said third party.

Relations with its outsourcer or provider relating to the applicant's information system are governed by a contract which the content is specified in AMF Position-Recommendation DOC-2020-07.

3. GENERAL REQUIREMENTS APPLICABLE TO ALL SERVICES EXCEPT THE SERVICE OF ADVICE TO INVESTORS IN DIGITAL ASSETS

3.1. CYBERSECURITY PROGRAMME

The applicant must define, formalize, implement and monitor an ongoing cybersecurity program aimed at controlling the level of security of the information systems involved in the provision of the digital assets service(s).

This program must in particular:

1°) include at least the items mentioned in this section 3.1;

2°) be constituted as internal security policies and validated by management bodies and based on the topics and chapters of the ISO 27002 standard. These policies must be formalised, verified and audited. They must be reviewed and updated, if necessary, at least once a year, or if an event occurs that so warrants.
However, the applicant is not required to have ISO 27001 certification.

The applicant must appoint an information systems security manager responsible for implementing the cybersecurity program with a sufficiently senior reporting line and provide his or her contact details to the AMF.

3.1.1 Cyber risks analysis

As early as the design phase, an analysis of security risks that could have a negative impact on the confidentiality, integrity, availability and traceability (CIAT) of information systems.
This analysis must enable to identify and assess the probability and impact of net and residual risks, as well as to identify the security measures needed to control them. It must also provide a representation of the risks in matric form, on two orthogonal axes, representing the probability and impact axes.
Critical information systems, security services and sensitive data assessed in relation to CIAT criteria must be specifically listed, and those working on them must be specifically made aware of this risk.

Operational scenarios involving physical threats to people with functional or technical privileges, or to components providing access to digital assets or legal tender, are taken into account in the risk analysis.

The EBIOS Risk Manager document (see EBIOS) provides a method for risk analysis.

3.1.2. Analysis of the Privacy Impact Assessment (PIA)

This analysis must make it possible to assess the level of risk generated by the treatment for the rights and freedoms of physical individuals and to provide appropriate measures to mitigate this risk. The applicant must also ensure that its processing operations comply with European Regulation No. 2016/679, known as the General Data Protection Regulation (GDPR), in particular regarding compliance with obligations relating to subcontracting and the rules governing the international transfer of personal data.

3.1.3. Preventive measures

The implementation of human, organizational and technical resources to control identified risks and meet defined availability integrity, confidentiality and traceability requirements.

The following guides may be used as reference:

1. the ANSSI computer hygiene guide (see HYGANSSI);
2. the CNIL personal data security guide (see SECCNIL);
3. the initial findings of the CNIL's analysis with regard to Blockchain technology (see BLCNIL).

3.1.4. Control systems

Systems to monitor the presence and effectiveness of the security measures identified in advance.
These control systems must be made up of different, mutually independent lines of defense, from the operational teams to the internal inspection/audit team. These control systems are made up of three mutually independent lines of defense, namely: (i) the operational teams; (ii) the compliance and risk team; and the inspection/internal audit team.

3.1.5. Review of user accounts and associated rights

Policies and procedures for regular review of accounts and access rights on the information systems listed above.

3.1.6. Vulnerability management

Vulnerability management, including the monitoring of technical vulnerabilities and threats that may arise, and the application of a policy enabling them to be dealt with according to time commitments adapted to the criticality of the vulnerabilities identified.

3.1.7. Detection measures

The human and technical resources needed to detect intrusions or, more generally, feared events on the information systems listed above.

3.1.8. Response measure

Policies and procedures for responding to security incidents and ensuring nominal business resumption, including crisis management (see CRISEANSSI).

3.2. OPERATIONAL MEASURES

Recognising that, to date, almost all digital assets services are offered via a website and/or mobile application, this section aims to list general technical requirements to guarantee a minimum level of security.

3.2.1. Component security

The technical components involved in the provision of the service must be identified and kept up to date.

In addition, the list of dependencies must be controlled to ensure that there is confidence in the components deployed to provide the service.

The configuration of the technical components involved in the provision of the service must be made more robust in accordance with the risk analysis performed. The following guides may be referenced in relation to this requirement:

a. the ANSSI configuration and best practice guides (see BPANSSI);
b. the Center for Internet Security association's configuration guides (see CIS).

3.2.2. Application development security

Application development carried out by the applicant to provide its digital assets service must take into account the following application security guidelines:

a. The ANSSI's best practice guide to Web standards security (see WEBANSSI)
b. the OWASP Top 10 general recommendations (see OWASPR);
c. the current OWASP Top 10 for web application security (see OWASPW);
d. the current OWASP Mobile Top 10 for mobile application security (see OWASPM).

3.2.3. Authentication

3.2.3.1. Domain names

Domain names used to provide the digital assets service must be authenticated by the DNSSEC extension (see DNSSEC).

3.2.3.2. Technical services exposed to the internet

The applicant must authenticate the services it exposes to the internet by means of an X.509 certificate signed by a publicly recognized Certification Authority.

The applicant, when offering a service on a mobile application, must implement a certificate pinning security measure to provide strong authentication for the remote technical service (see PIN).

3.2.3.3. Users

By default, the applicant must allow users of its service to be authenticated using a second robust authentication factor (see PWANSSI) in addition to the usual password. A clear message informing users of the risks associated with not using two- factor authentication must be displayed, and their explicit consent must be obtained for them to waive this additional protection.

3.2.3.4. Administrators

The applicant must provide a strong, two-factor authentication mechanism for use by technical and functional administrators of the information system(s) (seePWANSSI).

3.2.4. Encryption

3.2.4.1. Communications

The communication flows involved in providing and administering the service must be systematically encrypted using robust encryption protocols and algorithms in accordance with the following guidelines for selecting the protocols and algorithms to be used: Annex B1 of the GSR (see RGSB1) and the ANSSI guide relating to the TLS protocol flow encryption (see TLSANSSI).
Rather than developing their own solutions, applicants are strongly encouraged to use proven implementations with security monitoring.

3.2.4.2. Data

The applicant must guarantee that users have protection in terms of the confidentiality and integrity of their data. This guarantee must not be based solely on boundary protection for the service provided and must cover more generally the risk of intrusion into the service by an attacker in a logic of defense in depth.

3.3. ELECTRONIC WALLET SECURITY

The applicant must advise, in writing, its clientsto use electronic wallets with state-of-the-art level security, such as the use of:

a. protection by password or encryption key; and/or

b. the encryption of secrets, including the private key, in accordance with technical recommendations in Annex B1 of the GSR (see RGSB1); and/or

c. offline storage.

3.4. DLT SECURITY

Where a distributed ledger technology (DLT) designed by the applicant itself or by one of its suppliers is used for the purposes of the required service, the AMF may require it to be certified under a recognised security scheme (such as at least First Level Security Certification (see CSPN) or Common Criteria Certification (see CCC)). This possibility is especially important because the DLT is private, is based on proprietary technology or uses code that is not available as open source.

3.5. SECURITY INCIDENT REPORTING

Following the occurrence of a significant security incident involving a digital assets service, the applicant must immediately inform the AMF by issuing a summary report that includes: the date of occurrence of the incident and the chronology of events;

a. the nature of the incident;
b. the scope of the issue;
c. the digital assets service(s) impacted;
d. the impact of the incident, on the systems and for the users of the service;
e. the method and chronology of detection;
f. the results of any investigation carried out;
g. the proposed action plan for remedying the incident;
h. the measures taken to prevent a similar incident from happening again in the future;
i. any other relevant information related to the incident.

4. SPECIFIC REQUIREMENTS APPLICABLE TO THE DIGITAL ASSETS CUSTODY SERVICE ON BEHALF OF THIRD PARTIES

As part of this service, the applicant can move digital assets in particular in two usage scenarios:

a) It generate and operate an electronic wallet dedicated to the client or an electronic wallet containing the digital assets of the client among other digital assets; or

(b) It holds access means, entrusted by the customer, enabling to move the customer's digital assets (for instance, an API key).

4.1. REQUIREMENTS COMMON TO BOTH USAGE SCENARIOS

The procedures for generating, storing, saving, responding to compromised keys or secrets used to generate keys (seeds), returning and destroying electronic wallets must be formalized, verified and regularly audited.

The offline storage of wallets is preferred because it limits the risk of their being compromised.

4.2. PRODUCTION OF THE WALLET

When creating a hierarchical deterministic wallet, the seed and private key must be securely backed up using appropriate means and access to them must be monitored and logged.
The multi-signature feature is preferred for creating a wallet because it requires a quorum (user, applicant, etc.) to sign a transaction.

4.3. CUSTODY OF THE MEANS OF ACCESS FOR THIRD PARTIES

It is forbidden to store authentication data from customer’s user account to a third-party service providing access to digital assets (login and password, temporary double authentication code, etc.).

5. REQUIREMENTS APPLICABLE FOR THE SERVICES OF BUYING OR SELLING DIGITAL ASSETS FOR LEGAL TENDER, OF TRADING DIGITAL ASSETS FOR OTHER DIGITAL ASSETS , OF OPERATION OF A DIGITAL ASSET TRADING PLATFORM AND OF RECEPTION AND TRANSMISSION OF ORDERS FOR DIGITAL ASSETS ON BEHALF OF THIRD PARTIES

When the applicant is applying for reinforced registration or a license for the service(s) of buying or selling digital assets in legal tender,
exchanging digital assets for other digital assets, operating a digital asset trading platform and/or receiving and transmitting orders in digital assets on behalf of third parties, without providing a digital asset custody service on behalf of third parties, the applicant shall not hold digital assets or means for accessing to digital assets that belongs to the client:

a. only the client's public key can be stored on the platform providing the service;

b. the client must therefore have his or her own e-wallet solution for sending or receiving the digital assets bought or sold.

If the applicant, in order to provide its service, requires that the client transfer digital assets to a deposit wallet controlled by the applicant, then the applicant effectively holds assets belonging to the user and must therefore comply with the specific security requirements applicable to the digital asset custody service on behalf of third parties defined in paragraph 4.

6. SPECIFIC REQUIREMENTS APPLICABLE TO THE SERVICE OF MANAGING DIGITAL ASSETS PORTFOLIOS ON BEHALF OF THIRD PARTIES

The applicant applying for license for providing a digital assets portfolio management service (here and after referred as the "agent") must, for each user of its service (here and after referred to as the "client"), create an electronic wallet dedicated to managing the client's digital assets:

a. whose private key is generated by the agent and is not sent to or known by the client;

b. that is operated by the agent using an e-wallet solution that complies with the requirements of Chapters 3.3 and 4.2.

Upon termination of the management contract, the agent must not communicate to the client the electronic wallet's private key used during the contract, but must instead return the assets to the client via an appropriate transfer service.

The purpose of these provisions is to ensure the strict accountability of management activities carried out by the agent on the client's electronic wallet(s) during and after termination of the management contract.

However, if the applicant performs the management activities directly on the client's personal wallet of digital assets it must:

a) comply with the specific security requirements applicable to the digital assets custody service on behalf of third parties, defined in paragraph 4;
b) make specific contractual arrangements with the client to define the sharing of responsibilities in the event of fraudulent use of the means of access to the digital assets by one of the parties.

7. CONTENTS OF THE REGISTRATION OR LICENCE FILE

The application file to be submitted to the AMF includes the following items:

1) A self-assessment of compliance with the cybersecurity requirements described in this Instruction;
2) A cyber-risk analysis, in accordance with the requirements set out in paragraph 3.1.1 of this Instruction;
3) An IT resources mapping document listing the IT resources used, the associated organizational arrangements, their criticality for the applicant, the interactions between resources, and the cyber risk control arrangements for these resources;
4) An audit report produced by one or more third parties with the PASSI qualification provided by ANSSI, covering the following scopes (see PASSI) :
    a. organizational and physical audit,
    b. configuration audit,
    c. intrusion testing, at least in black and gray boxes,
    d. code review, if the applicant uses or develops smart contracts.

Audits must be carried out within the framework and conditions of PASSI qualification.

They must cover the perimeter of the internal or external information system involved in the provision of the digital asset service(s) for which approval or enhanced registration is requested.

The PASSI auditor must help the applicant to define the scope to be audited by:
- drawing on documents 2) and 3);
- listing the systems which, as a cybersecurity professional, he or she considers critical or important in terms of security requirements (CIAT), and with regard to the intrinsic risks of the business activity planned by the applicant. For example, the custody of digital assets is a critical service by its very nature;
- It also includes systems supporting the requester's cross-functional processes, which are often targeted by attackers and then bounced back onto business systems: messaging systems, directories, workstations, mobile terminals, etc.

The applicant must attach to the audit report a document formalized by its information systems security manager, and validated by the applicant's governing bodies, setting out the action plan and timetable for remedying the risks and findings identified in the audit report.

The document(s) making up the audit report produced by the third-party auditor must:

a) comply with the formalization requirements of chapter VI.6 of the PASSI (see PASSIR) standard;
b) incorporate a risk-based approach, in particular by representing risks in matrix form, on two orthogonal axes, and evaluating the probability and impact criteria for the risks identified;
c) be electronically signed by the third-party auditor.

When the AMF asks the applicant to use evaluated and certified products, the applicant must provide the AMF with the certificate issued under the conditions set out by Decree No. 2002-535 of April 18, 2002, in accordance with Article 721-4 of the RGAMF.

The AMF may request additional information (policies, procedures, control plans, etc.).

Annex: Document References

Reference	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
[CRISEANSS]	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/guide/cryptographie-les-regles-du-rgs/
[WEBANSSI]	https://www.ssi.gouv.fr/administration/guide/recommandations-pour-la-securisation-des-sites-web/