AMF INSTRUCTION

DOC-2019-24

DIGITAL ASSETS SERVICE PROVIDERS – CYBERSECURITY SYSTEM OF REQUIREMENTS

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

1. INTRODUCTION

1.1. OVERVIEW

1.1.1. Background

Pursuant to Article L. 54-10-5 of the French Monetary and Financial Code ("MFC"), the services providers established in France may, 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 licence.

In order to obtain the licence, Article D. 54-10-6 of the MFC provides that the applicant forward to the AMF the information relating to its organisation, which the content is specified into the AMF General Regulation.

Article 721-4 of the AMF General Regulation refers to the security of information systems, also known as "cybersecurity", with which the applicant must comply:

"When the AMF asks the applicant to use evaluated and certified products or to have security audits performed in application of Articles D. 54-10-7 and D. 54-10-9 of the Monetary and Financial Code, the product evaluation and security audit are performed in accordance with an instruction on the system of requirements."

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;
- personal data breaches;
- denial of service attacks;
- identity theft;
- inability to investigate in the event of an incident or fraudulent activity.

1.1.2. Document purpose

The purpose of this document is to detail the requirements of the AMF under Article 721-4 of the AMF General Regulation for each digital assets service, for which the applicant may request a license. The request to be submitted to the AMF 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 licence is/are defined in Article D. 54-10-1 of the MFC.

An **applicant** refers to an organisation, whether public or private, seeking to obtain AMF 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 licensed digital assets services provider remains, in any event, fully accountable for the cybersecurity of the digital assets service for which it is licensed even if it outsources only a part of its system.

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 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, formalise, implement and monitor an ongoing cybersecurity programme aimed at controlling the level of security of the information systems involved in the provision of the digital assets service(s). This programme must include in particular:

1°) from the design phase, the analysis of security risks that could negatively impact the availability, integrity, confidentiality and traceability (AICT) of information systems. This analysis must make it possible to identify and assess the probability and impact of these risks, and identify the security measures required to manage them. Critical information systems, security services and sensitive data assessed in relation to the AICT criteria must be specifically listed and those involved in them must be specifically made aware of them;

2°) 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°) the implementation of human, organisational and technical resources to manage the risks identified and comply with the defined availability, integrity, confidentiality and traceability requirements;

4°) the systems for monitoring the existence and effectiveness of previously identified security measures;

5°) procedures for regularly reviewing the accounts and access rights for the information systems listed above;

6°) vulnerability management, including monitoring technical vulnerabilities and threats that may arise and implementing a policy to address them;

7°) the human and technical means for intrusion detection or, more generally, unexpected events on the information systems listed above;

8°) security incident response procedures and the resumption of normal operations.

To this end, the following guides may be used as reference:

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

In addition, the EBIOS Risk Manager document (see EBIOS) provides a method for risk analysis.

The applicant's internal policies relating to the topics and chapters of ISO 27002 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 programme and provide his or her contact details to the AMF.

3.2. OPERATIONAL MEASURES

Recognising that, to date, almost all digital assets services are offered via a website 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 OWASP Top 10 general recommendations (see OWASPR);
b. the current OWASP Top 10 for web application security (see OWASPW);

c. 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 recognised Certification Authority.

The applicant, when providing 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 authentication factor 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).

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).
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.

3.3. ELECTRONIC WALLET SECURITY

The applicant must advise 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 a 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 AUDIT

When the AMF requires a security audit, the audit must be performed according to the following conditions:

1) within the scope of the information system (whether internal or external) used to provide the digital assets service(s) for which it holds a license issued by the AMF;
2) by one or more third parties holding the PASSI information systems security audit providers' qualification (see PASSI) provided by the ANSSI, to cover at least the following areas:

a) organisational and physical audit;
b) architecture audit;
c) configuration audit;
d) penetration testing.

These audits must be carried out within the framework and under the conditions of the PASSI qualification.

The applicant must attach to the audit report a document formalised by its information systems security manager and presented to the applicant's management bodies, explaining the proposed action plan for remedying the risks and findings identified in the audit report.

The document(s) comprising the audit report prepared by the third party auditor must:

a. comply with the formalisation requirements of Chapter VI.6 of the PASSI reference document (see PASSIR);
b. incorporate a risk-based approach, in particular by presenting risks in a matrix format;
c. be signed electronically by the third party.

3.6. 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:

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

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

The primary objective of this service is to hold client positions on a consolidated basis, for example, in the context of the use of several types of assets or several DLTs.

To do this, the applicant can move digital assets in two usage scenarios:

a) It has the ability to move the client's digital assets, for example, by operating an electronic wallet dedicated to the client or an electronic wallet containing the digital assets of the client among other digital assets;b) It holds the private cryptographic keys of the client, i.e. its electronic wallet.

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 formalised, 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 PRIVATE KEYS FOR THIRD PARTIES

Apart from the wallet of the client, the custody of any other means of access to digital assets is prohibited, for example, authentication to a third party service that allows access to the wallet (login and password, etc.).

5. REQUIREMENTS APPLICABLE TO APPLICANTS FOR A LICENCE 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 registration 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 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, using the client's private key, 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.

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
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/