Seqlense

Guidelines de l'ESMA - Normes de l'Union sur la maintenance des systèmes et des protocoles d'accès à la sécurité liés aux crypto-actifs.

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Final Report - Guidelines specifying Union standards on the maintenance of systems and security access protocols for offerors and persons seeking admission to trading of crypto-assets other than asset referenced tokens and e-money tokens

Le règlement sur les marchés de crypto-actifs (MiCA) a été publié le 9 juin 2023 et l'ESMA a été mandatée pour élaborer des normes techniques et des lignes directrices conformément à l'article 14, paragraphe 1, afin de préciser les dispositions relatives à la maintenance des systèmes et des protocoles d'accès à la sécurité pour les offreurs de crypto-actifs. L'ESMA a consulté le groupe des parties prenantes du Securities and Markets Stakeholder Group ainsi que d'autres parties prenantes.

Le contenu du rapport de l'ESMA est le suivant :

Section II : Base juridique, résumé des commentaires des parties prenantes et justification des mises à jour des lignes directrices, y compris l'affinement des définitions pour les aligner sur les normes de l'Union.

Section II : Annexes :

Annexe I : Analyse coûts-avantages.
Annexe II : Retour d'information sur la consultation.
Annexe III : Lignes directrices finales.

L'objectif de ces lignes directrices de l'ESMA est de spécifier les normes de l'Union pour la maintenance des systèmes et des protocoles de sécurité. Elles s'appliquent aux autorités compétentes et aux « offerors (offrants) » tels que définis dans la MiCA, ainsi qu'aux personnes cherchant à être admises à la négociation de crypto-actifs autres que les jetons référencés par des actifs ou les jetons de monnaie électronique.

En ce qui concerne le principe de proportionnalité, les entités devraient se conformer aux lignes directrices de l'ESMA d'une manière qui soit proportionnée à leur taille, à leur profil de risque global, ainsi qu'à la nature, à l'étendue et à la complexité de leurs activités. Ce principe garantit la flexibilité, compte tenu de l'échelle variable des opérations des offrants. Ils doivent assurer une gouvernance interne et des cadres de contrôle adéquats pour maintenir les réseaux et les systèmes d'information et atténuer les risques liés aux TIC. Il convient également de définir clairement les rôles et les responsabilités des fonctions de gestion des risques liés aux TIC, y compris la formation du personnel aux risques liés aux TIC, et de veiller à ce que les compétences du personnel et les ressources budgétaires soient suffisantes pour soutenir la gestion des risques liés aux TIC. La direction doit superviser les dispositions prises en matière de gestion des risques liés aux TIC, et des mesures d'atténuation doivent être prises pour faire face aux risques liés aux fournisseurs de services TIC tiers.

Seqlense

Guidelines de l'ESMA - Normes de l'Union sur la maintenance des systèmes et des protocoles d'accès à la sécurité liés aux crypto-actifs.

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Des mesures de sécurité physique doivent être mises en œuvre pour protéger les locaux, les centres de données et toutes les zones sensibles contre les accès non autorisés et les risques environnementaux. L'accès physique aux réseaux et aux systèmes d'information doit être réservé aux personnes autorisées. Les entités doivent tenir des registres des accès aux zones sensibles et réexaminer périodiquement les droits d'accès.

L'accès logique aux réseaux et aux systèmes d'information doit également être limité aux personnes autorisées, avec des contrôles stricts de l'accès privilégié aux systèmes. L'accès aux systèmes doit être limité selon le principe du moindre privilège et de l'authentification forte. Il est recommandé de conserver les journaux d'accès pendant une période appropriée et de réexaminer périodiquement les droits d'accès, et l'accès aux systèmes privilégiés doit être étroitement contrôlé. Les entités doivent également utiliser les journaux d'accès pour détecter et enquêter sur les activités inhabituelles.

Les entités sont responsables de la gestion des clés cryptographiques tout au long de leur cycle de vie, notamment en ce qui concerne, entre autres, la génération, le renouvellement, le stockage, la révocation et la destruction. Des contrôles doivent être mis en œuvre pour les protéger contre la perte, l'accès non autorisé, la divulgation et la modification. Des méthodes doivent également être élaborées pour remplacer les clés cryptographiques en cas de perte, de compromission ou de détérioration. Un registre de tous les certificats critiques doit être tenu et mis à jour régulièrement.

Les lignes directrices de l'ESMA s'alignent sur des cadres tels que DORA, la directive NIS2 et les normes ISO afin de garantir la cohérence des TIC et des pratiques de gestion de la sécurité. Les offrants et les personnes cherchant à se faire admettre à la négociation doivent s'efforcer de se conformer à ces lignes directrices, dont la mise en œuvre est supervisée par les autorités compétentes. Les dispositions spécifiques sont adaptées pour refléter les exigences moins étendues pour les offrants que pour les CASP.

Prochaines étapes : Les lignes directrices seront traduites dans toutes les langues officielles de l'UE et publiées sur le site web de l'ESMA. Après la publication, les ANC auront deux mois pour notifier à l'AEMF leur conformité ou leur intention de se conformer.

Les lignes directrices entreront en vigueur trois mois après la publication des traductions.

Sources : (en anglais)
https://www.esma.europa.eu/document/final-report-guidelines-specifying-union-standards-maintenance-systems-and-security-access
https://www.esma.europa.eu/press-news/esma-news/esma-releases-last-policy-documents-get-ready-mica

Seqlense

ESMA Guidelines – Union standards on the maintenance of systems and security access protocols related to crypto-assets.

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

The Markets in Crypto-Assets Regulation (MiCA) was published on 9 June 2023 and ESMA was mandated to develop technical standards and guidelines in accordance with Article 14(1) to specify provisions regarding the maintenance of systems and security access protocols for crypto-asset offerors. The Securities and Markets Stakeholder Group as well as other stakeholders were consulted by ESMA.

The content of the ESMA report is as follows:

Section II: Legal basis, summary of the stakeholders' feedback, and the rationale for updates to the guidelines, including refining definitions to align with Union standards.

Section II: Annexes:

- Annex I: Cost-benefit analysis.
- Annex II: Feedback from the consultation.
- Annex III: Final guidelines.

The aim of these ESMA guidelines is to specify Union standards for maintaining systems and security protocols. They apply to competent authorities and to "offerors" as defined in MiCA, as well as persons seeking admission to trading of crypto-assets other than asset-referenced tokens or e-money tokens.

In reference to the proportionality principle, entities should comply with the ESMA guidelines in a way that is proportionate to their size, overall risk profile, and the nature, scope, and complexity of their activities. This principle ensures flexibility, considering the varying scale of offeror operations. They must ensure adequate internal governance and control frameworks to maintain network and information systems and mitigate ICT risks. Clear roles and responsibilities for ICT risk management functions should also be established, including staff training on ICT risks, and staff skills and budget resources should be adequate to support ICT risk management. Management oversight of ICT risk management arrangements is expected, as well as mitigation measures that should address risks from third-party ICT service providers.

Physical security measures should be implemented to protect premises, data centres, and all sensitive areas from unauthorised access and environmental hazards. Physical access to network and information systems should only be restricted to authorised individuals. Entities should keep logs of access to sensitive areas and periodically review access rights.

Logical access to networks and information systems should also be restricted to authorised individuals with strong controls over privileged system access. System access should be limited based on the principle of least privilege and strong authentication. It is recommended that access logs be retained for an appropriate period and that access rights be periodically reviewed, and privileged system access must be tightly controlled. Entities should also use access logs to detect and investigate unusual activities.

Seqlense

ESMA Guidelines – Union standards on the maintenance of systems and security access protocols related to crypto-assets.

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Entities are responsible for managing cryptographic keys throughout their lifecycle, among others, generation, renewal, storage, revocation, and destruction. Controls should be implemented to protect them against loss, unauthorized access, disclosure, and modification. Methods should also be developed to replace cryptographic keys in case of loss, compromise, or damage. A register for all critical certificates must be maintained and updated regularly.

The ESMA guidelines align with frameworks such as DORA, NIS2 Directive, and ISO standards to ensure consistency in ICT and security management practices. Offerors and persons seeking admission to trading are expected to make every effort to comply with these guidelines, whose implementation is supervised by competent authorities. Specific provisions are tailored to reflect the less extensive requirements for offerors compared to CASPs.

Next Steps: The guidelines will be translated into all official EU languages and published on the ESMA website. Following publication, NCAs will have two months to notify ESMA of their compliance or intent to comply.

The guidelines will become effective three months after the translations are published.

Sources:
https://www.esma.europa.eu/document/final-report-guidelines-specifying-union-standards-maintenance-systems-and-security-access
https://www.esma.europa.eu/press-news/esma-news/esma-releases-last-policy-documents-get-ready-mica