cssf

Commission de Surveillance
du Secteur Financier

Circulaire CSSF 25/889

Application des Orientations de l'ESMA concernant la spécification des normes de l'Union relatives à la maintenance des systèmes et des protocoles d'accès de sécurité pour les offreurs et les personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs et des jetons de monnaie électronique (ESMA75-223375936-6132)

Circulaire CSSF 25/889

Application des Orientations de l'ESMA concernant la spécification des normes de l'Union relatives à la maintenance des systèmes et des protocoles d'accès de sécurité pour les offreurs et les personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs et des jetons de monnaie électronique (ESMA75-223375936-6132)

À tous les offreurs au sens de l'article 3, paragraphe 1, point 13), du règlement (UE) 2023/1114[1] (« **règlement MiCA** »), ainsi qu'aux personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs ou des jetons de monnaie électronique tels que définis à l'article 3, paragraphe 1, points 6) et 7), du règlement MiCA.

Luxembourg, le 30 avril 2025

Mesdames, Messieurs,

L'objet de la présente circulaire est de porter à votre attention l'application, par la CSSF, en sa qualité d'autorité compétente, des Orientations de l'Autorité européenne des marchés financiers (« ESMA ») concernant la spécification des normes de l'Union relatives à la maintenance des systèmes et des protocoles d'accès de sécurité pour les offreurs et les personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs et des jetons de monnaie électronique (ESMA75-223375936-6132), (« Orientations »), publiées le 26 février 2025. La CSSF a ainsi intégré ces Orientations dans sa pratique administrative et dans son approche réglementaire en vue de favoriser la convergence en matière de surveillance dans ce domaine au niveau européen.

1. Les Orientations

Les Orientations sont émises par l'ESMA sur la base de l'article 14, paragraphe 1, point d), du règlement MiCA conformément à l'article 16 du règlement (UE) n° 1095/2010.

Les Orientations s'appliquent à compter du 27 avril 2025.

Les Orientations, élaborées en coopération avec l'Autorité bancaire européenne, sont fondées sur l'article 14, paragraphe 1, point d), du règlement MiCA. Elles ont pour objet de préciser les normes de l'Union applicables aux offreurs et personnes qui demandent l'admission à la négociation en ce qui concerne la maintenance des systèmes et des protocoles d'accès de sécurité, y compris les politiques et procédures. Elles visent également à rendre plus uniformes l'interprétation et l'application des dispositions du règlement MiCA applicables aux offreurs et aux personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs et des jetons de monnaie électronique.

[1] Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) n° 1093/2010 et (UE) n° 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937

Les Orientations sont annexées à la présente circulaire et disponibles sur le site Internet de l'ESMA https://www.esma.europa.eu/.

2. Champ d'application

La présente circulaire s'applique aux offreurs au sens de l'article 3, paragraphe 1, point 13), du règlement MiCA, ainsi qu'aux personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs ou des jetons de monnaie électronique tels que définis à l'article 3, paragraphe 1, points 6) et 7), du règlement MiCA.

3. Date d'application

La présente circulaire s'applique à compter du 27 avril 2025.

Claude WAMPACH
Directeur

Marco ZWICK
Directeur

Jean-Pierre FABER
Directeur

Françoise KAUTHEN
Directeur

Claude MARX
Directeur général

Annexe Orientations de l'ESMA concernant la spécification des normes de l'Union relatives à la maintenance des systèmes et des protocoles d'accès de sécurité pour les offreurs et les personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs et des jetons de monnaie électronique (ESMA75-223375936-6132)

26/02/2025
ESMA75-223375936-6132

Orientations

Concernant la spécification des normes de l'Union relatives à la maintenance des systèmes et des protocoles d'accès de sécurité pour les offreurs et les personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs et des jetons de monnaie électronique

Table des matières

1 Champ d’application

Qui ?

1. Les présentes orientations s’appliquent aux autorités compétentes et aux «offreurs» au sens de l’article 3, paragraphe 1, point 13, du règlement MiCA, ainsi qu’aux personnes qui demandent l’admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs ou des jetons de monnaie électronique.

Quoi ?

2. Les présentes orientations s’appliquent en rapport avec l’article 14, paragraphe 1, point d), du règlement MiCA.

Quand ?

3. Les présentes orientations commencent à s’appliquer 60 jours civils à compter de la date de leur publication sur le site internet de l’ESMA dans toutes les langues officielles de l’UE.

2 Références législatives, abréviations et définitions

2.1 Références législatives

Directive SRI2	Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148[1].
DORA	Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014, (UE) nº 909/2014 et (UE) 2016/1011[2].
MiCA	Règlement (UE) 2023/1114 du Parlement européen et du Conseil du 31 mai 2023 sur les marchés de crypto-actifs, et modifiant les règlements (UE) nº 1093/2010 et (UE) nº 1095/2010 et les directives 2013/36/UE et (UE) 2019/1937[3].
Règlement instituant l'ESMA	Règlement (UE) nº 1095/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité européenne des marchés financiers), modifiant la décision nº 716/2009/CE et abrogeant la décision 2009/77/CE de la Commission[4].

2.2 Abréviations

ART	Jeton(s) se référant à un ou des actifs
CE	Commission européenne
EMT	Jeton(s) de monnaie électronique
ESMA	European Securities and Markets Authority (AEMF – Autorité européenne des marchés financiers)
UE	Union européenne

[1] JO L 333 du 12.12.2022, p. 80.
[2] JO L 333 du 14.12.2022, p. 1.
[3] JO L 150 du 9.6.2023, p. 40.
[4] JO L 331 du 15.12.2010, p. 84.

2.3 Définitions

Actif de TIC	s'entend d'un « actif de TIC » (au sens de l'article 3, point 7, du règlement DORA.
Contrôle des accès	s'entend des contrôles visant à garantir que l'accès physique et logique aux actifs de TIC est autorisé et limité en fonction des exigences de sécurité de l'entreprise et de l'information[5].
Offreurs et personnes qui demandent l'admission à la négociation	fait référence à la forme abrégée du terme «offreurs et personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à un ou des actifs et des jetons de monnaie électronique», aux fins des présentes orientations.
Réseau et système d'information	s'entend d'un « réseau et système d'information » au sens de l'article 6, point 1, de la directive SRI2.
Risque lié aux TIC	s'entend d'un « risque lié au TIC » au sens de l'article 3, point 5, du règlement DORA.

3 Objet

4. Les présentes orientations, élaborées en coopération avec l'Autorité bancaire européenne, sont fondées sur l'article 14, paragraphe 1, point d), du règlement MiCA. Elles ont pour objet de préciser les normes de l'Union applicables aux offreurs et personnes qui demandent l'admission à la négociation en ce qui concerne la maintenance des systèmes et des protocoles d'accès de sécurité, y compris les politiques et procédures. Elles visent également à rendre plus uniformes l'interprétation et l'application des dispositions du règlement MiCA applicables aux offreurs et aux personnes qui demandent l'admission à la négociation.

[5] *ISO/IEC 29146:2016 Technologies de l'information - Techniques de sécurité — Cadre pour la gestion de l'accès*. Organisation internationale de normalisation, 2016.

4 Obligations en matière de conformité et de déclaration

4.1 Statut des orientations

5. Conformément à l'article 16 du règlement instituant l'ESMA, les autorités compétentes mettent tout en œuvre pour surveiller l'application des présentes orientations, et les offreurs ou les personnes qui demandent l'admission à la négociation devraient tout mettre en œuvre pour s'y conformer.

6. Les autorités compétentes auxquelles les présentes orientations s'appliquent devraient les intégrer à leur cadre juridique et/ou de surveillance national, le cas échéant, y compris lorsque certaines orientations données visent en premier lieu les acteurs du marché des crypto-actifs relevant de leur compétence. Dans ce cas, les autorités compétentes devraient, par leur surveillance, veiller à ce que les acteurs des marchés financiers se conforment aux orientations.

4.2 Exigences de déclaration

7. Dans un délai de deux mois à compter de la date de la publication des présentes orientations sur le site internet de l'ESMA dans toutes les langues officielles de l'UE, les autorités compétentes auxquelles s'appliquent ces orientations devraient notifier à l'ESMA si elles i) se conforment, ii) ne se conforment pas, mais entendent se conformer, ou iii) ne se conforment pas et n'entendent pas se conformer aux orientations.

8. En cas de non-conformité, les autorités compétentes doivent aussi notifier à l'ESMA les raisons pour lesquelles elles ne s'y conforment pas, en faisant cette notification dans un délai de deux mois à compter de la date de publication des orientations sur le site web de l'ESMA dans toutes les langues officielles de l'UE.

9. Un formulaire de notification est disponible sur le site internet de l'ESMA. Une fois le formulaire complété, il doit être transmis à l'ESMA.

10. Les offreurs et personnes qui demandent l'admission à la négociation ne sont pas tenus de déclarer s'ils se conforment ou non aux présentes orientations.

5 Orientations précisant les normes de l'Union relatives à la maintenance des systèmes et des protocoles d'accès de sécurité pour les offreurs et les personnes qui demandent l'admission à la négociation de crypto-actifs autres que des jetons se référant à des actifs et des jetons de monnaie électronique

5.1 Orientation nº 1 : Principe général de proportionnalité

11. Les offreurs et les personnes qui demandent l'admission à la négociation sont tenus de tout mettre en œuvre pour respecter les présentes orientations d'une manière qui soit proportionnée à la taille de l'organisation, à son profil de risque global, ainsi qu'à la nature, à la portée et à la complexité de ses activités ou opérations.

5.2 Orientation nº 2 : Dispositions administratives concernant les systèmes et les protocoles d'accès de sécurité

Dispositions administratives

12. L'offreur ou la personne qui demande l'admission à la négociation devrait garantir la mise en place d'un cadre approprié de gouvernance et de contrôle internes pour la maintenance de ses réseaux et systèmes d'information et l'atténuation des risques liés aux TIC. L'offreur ou la personne qui demande l'admission à la négociation devrait également définir clairement les rôles et les responsabilités des fonctions chargées de la gestion des risques liés aux TIC.

13. L'offreur ou la personne qui demande l'admission à la négociation devrait veiller, en permanence, à ce que son personnel ait les compétences et les ressources budgétaires suffisantes pour soutenir les dispositifs de gestion des risques liés aux TIC, en particulier en ce qui concerne le personnel chargé de la maintenance des réseaux et des systèmes d'information ainsi que des contrôles des accès. En outre, l'offreur ou la personne qui demande l'admission à la négociation devrait veiller à ce que les membres du personnel concernés, y compris tout titulaire de postes clés, reçoivent périodiquement une formation appropriée sur les risques liés aux TIC.

14. L'organe de direction de l'offreur ou de la personne qui demande l'admission à la négociation devrait être responsable de la définition, de l'approbation et de la surveillance de la mise en œuvre des dispositifs de gestion des risques liés aux TIC de l'organisation, notamment en ce qui concerne son réseau et ses systèmes d'information, ainsi que les contrôles des accès.

Rôles et responsabilités

15. L'offreur ou la personne qui demande l'admission à la négociation devrait charger du personnel au sein de l'organisation de la tâche de déceler, gérer et surveiller de manière appropriée les risques liés aux TIC. Il devrait veiller à ce que le personnel chargé de la gestion des risques liés aux TIC et des opérations de sécurité ait des dispositifs appropriés pour détecter, suivre, évaluer et rendre compte de ces risques liés aux TIC.

16. L'offreur ou la personne qui demande l'admission à la négociation devrait veiller à ce que le personnel chargé de la gestion des risques liés aux TIC associés aux réseaux et systèmes d'information et aux contrôles des accès soit en mesure de garantir que les risques liés aux TIC décelés sont surveillés, évalués et communiqués à l'organe de direction.

17. L'offreur ou la personne qui demande l'admission à la négociation devrait définir et attribuer les principaux rôles et responsabilités afin de mettre en place des dispositifs visant :

    i. à déceler et à évaluer les risques liés aux TIC, notamment ceux liés aux services de TIC fournis par des prestataires de services tiers, auxquels l'organisation est exposée ;

    ii. à définir des mesures d'atténuation, y compris des contrôles permettant d'atténuer les risques liés aux prestataires tiers de services TIC ;

    iii. à contrôler l'efficacité des mesures visées au point ii) et, le cas échéant, à prendre des mesures correctives ;

    iv. à faire rapport à l'organe de direction sur les risques liés aux TIC et les mesures d'atténuation ;

    v. à déterminer et à évaluer s'il existe des risques liés aux TIC résultant d'un changement majeur dans les réseaux et les systèmes d'information ou les services TIC (notamment lorsque ceux-ci sont fournis par des tiers), ou à la suite d'un incident opérationnel ou de sécurité important ;

    vi. à gérer les clés cryptographiques tout au long de leur cycle de vie.

5.3 Orientation nº 3 : Protocoles d'accès de sécurité physiques

18. Les offreurs et les personnes qui demandent l'admission à la négociation devraient définir, consigner et appliquer des mesures de sécurité physiques afin de protéger leurs locaux, leurs centres de données et leurs zones sensibles contre tout accès non autorisé et contre les risques environnementaux. L'offreur ou la personne qui demande

l'admission à la négociation devrait tenir un registre de chaque entrée dans les locaux qui nécessitent une autorisation d'accès.

19. Seules les personnes autorisées devraient pouvoir accéder physiquement aux réseaux et aux systèmes d'information, conformément aux principes du besoin d'en connaître et du moindre privilège, et au cas par cas. L'autorisation devrait être attribuée conformément aux tâches et aux responsabilités de la personne autorisée et se limiter aux personnes qui bénéficient d'une formation et d'un suivi appropriés. Il convient de réévaluer de manière périodique l'accès physique et de le retirer aux personnes qui n'en ont plus besoin.

20. Les mesures appropriées de protection contre les dangers environnementaux devraient être proportionnées à l'importance des bâtiments et au caractère critique des opérations ou des réseaux et systèmes d'information qu'ils abritent.

5.4 Orientation nº 4 : Protocoles d'accès de sécurité pour les réseaux et les systèmes d'information

21. L'accès logique aux réseaux et aux systèmes d'information devrait être limité aux personnes autorisées désignées par l'offreur ou la personne qui demande l'admission à la négociation. L'autorisation devrait être attribuée conformément aux tâches et aux responsabilités du personnel et se limiter aux membres qui bénéficient d'une formation et dont l'accès aux systèmes fait l'objet d'une surveillance. Les offreurs et les personnes qui demandent l'admission à la négociation devraient mettre en place des contrôles fiables ne permettant qu'aux personnes ayant un besoin légitime professionnel d'accéder aux réseaux et systèmes d'information. L'accès électronique des applications aux données et aux systèmes devrait se limiter au strict nécessaire pour fournir le service pertinent.

22. Les offreurs et les personnes qui demandent l'admission à la négociation devraient instaurer des contrôles solides sur l'accès privilégié aux systèmes en limitant strictement et en supervisant étroitement le personnel bénéficiant de droits d'accès renforcés aux systèmes. Devraient être mis en œuvre des contrôles tels que l'accès basé sur les rôles, la journalisation et la revue des activités des réseaux et des systèmes d'information des utilisateurs privilégiés, une authentification renforcée et un suivi des anomalies. L'offreur ou la personne qui demande l'admission à la négociation devrait gérer les droits d'accès aux actifs informationnels et aux systèmes sous-jacents selon le principe du « besoin d'en connaître » et du moindre privilège. Les droits d'accès logique devraient être périodiquement réévalués et retirés lorsqu'ils ne sont plus nécessaires.

23. Les registres d'accès devraient être conservés pendant une période proportionnée au caractère critique des fonctions commerciales, des processus de soutien et des actifs informationnels en question, sans préjudice des obligations en matière de conservation

fixées par le droit de l'Union et le droit national. Les offreurs et les personnes qui demandent l'admission à la négociation devraient utiliser ces informations pour aider à identifier et instruire plus facilement les activités anormales qui ont été repérées dans le cadre de la fourniture de leurs services.

24. L'accès à distance par des administrateurs à des actifs de TIC essentiels ne devrait être accordé que selon le besoin d'en connaître et du moindre privilège, et uniquement lorsque des solutions d'authentification renforcée sont disponibles.

25. Le fonctionnement des produits, outils et procédures liés aux processus de contrôle des accès devrait protéger ces processus de contrôle des accès contre tout risque de violation ou de contournement, ce qui comprend l'enregistrement, la livraison, la révocation et le retrait des produits, outils et procédures correspondants.

5.5 Orientation nº 5 : Gestion des clés cryptographiques

26. L'offreur ou la personne qui demande l'admission à la négociation devrait être responsable de la gestion des clés cryptographiques dans le cadre des rôles et responsabilités attribués aux membres clés du personnel en matière de risques liés aux TIC. Ces membres du personnel de l'offreur ou de la personne qui demande l'admission à la négociation devraient être responsables de la gestion des clés cryptographiques tout au long de leur cycle de vie, à savoir leur génération, renouvellement, stockage, sauvegarde, archivage, récupération, transmission, retrait, révocation et destruction.

27. Les offreurs et les personnes qui demandent l'admission à la négociation devraient déterminer et mettre en œuvre des contrôles visant à protéger les clés cryptographiques tout au long de leur cycle de vie contre la perte, l'accès non autorisé, la divulgation et la modification.

28. Les offreurs et les personnes qui demandent l'admission à la négociation devraient élaborer et mettre en œuvre des méthodes afin de remplacer les clés cryptographiques si celles-ci sont perdues, compromises ou endommagées.

29. Les offreurs et les personnes qui demandent l'admission à la négociation devraient créer et tenir à jour un registre de tous les certificats et dispositifs de stockage de certificats pour au moins les actifs de TIC essentiels. Le registre devrait être tenu à jour.

30. Les offreurs et les personnes qui demandent l'admission à la négociation devraient assurer le renouvellement rapide des certificats avant leur expiration.