11 October 2024
ESMA35-1872330276-195

Opinion

On MiCA regulatory technical standards on the authorisations of crypto-asset service providers and notifications by certain financial entities to provide crypto-asset services

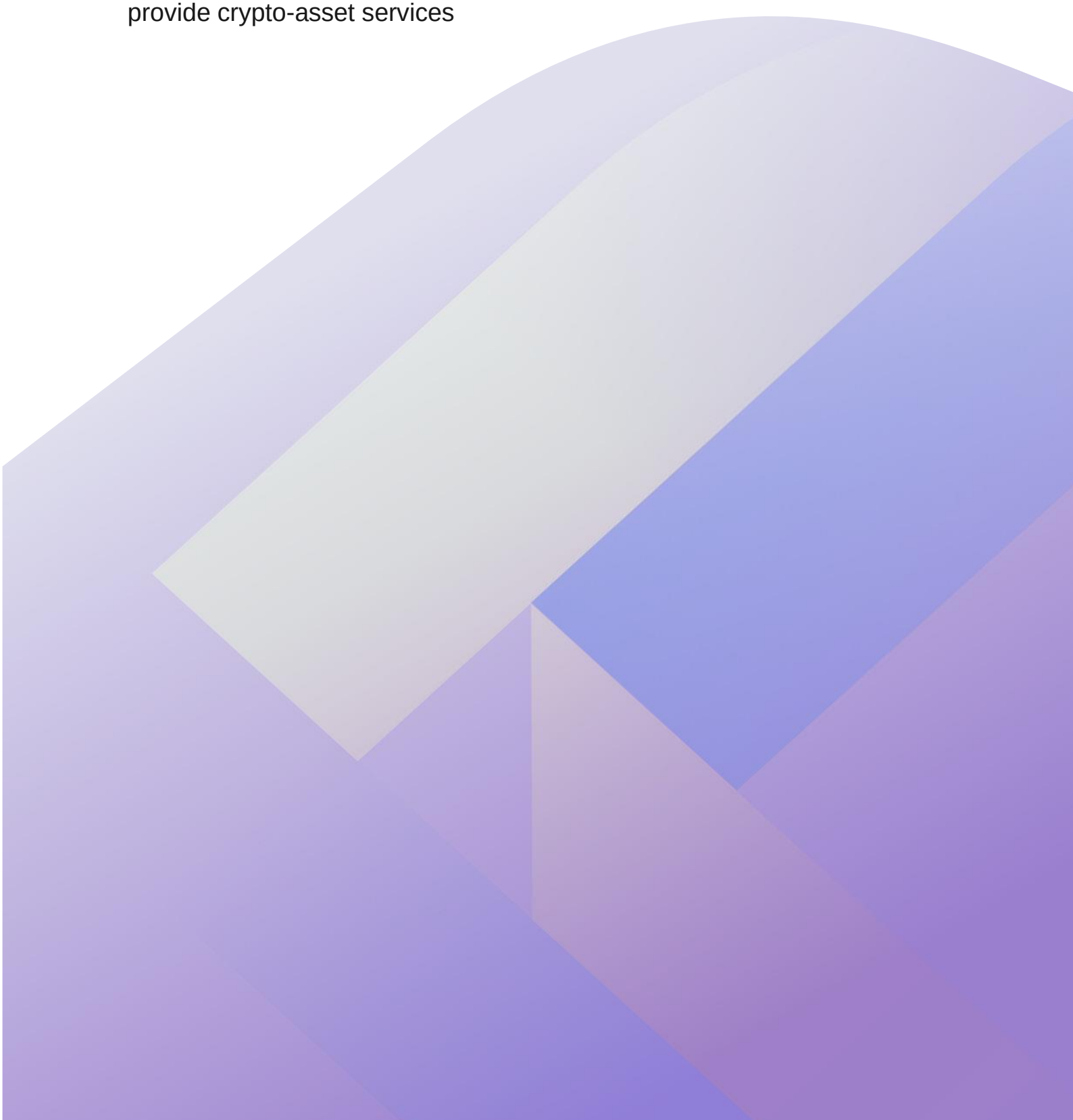

Table of Contents

1 Executive Summary

Reasons for publication

The Regulation on markets in crypto-assets (MiCA)[1] requires ESMA to submit draft regulatory technical standards (RTS) to further specify:

- the information to be included in a notification by certain financial entities of their intention to provide crypto-asset services (hereafter the "**draft RTS on notifications**"); and

- the information to be included in an application for authorisation as crypto-asset service provider (hereafter the "**draft RTS on authorisations**").

On 25 March 2024, ESMA published its first final report on draft technical standards specifying certain requirements of MiCA[2] and submitted it to the European Commission (the EC) for adoption[3].

On 3 September 2024, the EC sent two letters informing ESMA that it intends to adopt the two RTS with amendments, which were included in an Annex to the letters. The EC invited ESMA to submit new drafts of the two RTS reflecting the proposed amendments.

Pursuant to the ESMA Regulation, within a period of six weeks from the receipt of the letter, ESMA may amend the draft RTS and resubmit them to the EC in the form of a formal opinion.

In this opinion, ESMA takes note of the legal interpretation by the EC, limiting the mandates to ESMA in Articles 60(13) and 62(5) of MiCA. However, ESMA also reiterates the importance of the policy objectives pursued by its initial proposal to require a cybersecurity audit realised by a third-party cybersecurity auditor. To ensure that crypto-asset service providers are subject to a thorough screening process, including in relation to their ICT systems, prior to their entering into the crypto-assets market, ESMA would thus recommend that the Commission amends the level 1 text of the MiCA framework to include such a requirement for a cybersecurity audit realised by a third-party auditor at the time of the authorisation.

Contents

Section 2 describes the legal basis, Section 3 sets out the background, as well as the policy objectives and ESMA's position on the amendments proposed by the EC.

Next Steps

In response to the letters received on 3 September 2024, ESMA has adopted this opinion, which is being communicated to the EC, with copies to the European Parliament and the Council. The European Parliament and the Council may object to an RTS adopted by the EC within a period of three months.

[1] Regulation (EU) 2023/1114 of the European Parliament and the Council of 31 May 2023 on markets in crypto-assets (OJ L 150,9.6.2023, p. 40–205).
[2] ESMA18-72330276-1634 Final Report on Draft technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) – first package (europa.eu).
[3] Pursuant to Article 10(1) of Regulation (EU) No 1095/2010 (the 'ESMA Regulation').

2 Legal basis

1. MiCA provides that ESMA shall develop draft RTS to further specify:

   - the information referred to in Article 60(7) of MiCA, to be included in a notification by certain financial entities of their intention to provide crypto-asset services (Article 60(13) of MiCA);

   - the information referred to in Article 62(2) and (3) of MiCA, to be included in a application for authorisation as crypto-asset service provider (Article 62(5) of MiCA).

2. On 25 March 2024, ESMA published its first final report on draft technical standards specifying certain requirements of MiCA (including the draft RTS on notifications and the draft RTS on authorisations) and submitted it to the EC for adoption pursuant to Article 10(1) of the ESMA Regulation ((EU) No 1095/2010).

3. On 3 September 2024, ESMA received two letters from the EC[4] informing ESMA that it intends to adopt the 2 proposed RTS with amendments, which were included in an Annex to the letters, and invited ESMA to submit new draft RTS to the EC reflecting these amendments.

4. Pursuant to Article 10(1) of the ESMA Regulation, within a period of six weeks from the receipt of the EC's letters, ESMA may amend its draft RTS and resubmit them to the EC in the form of a formal opinion.

5. ESMA's competence to deliver an opinion is based on Article 10(1) of the ESMA Regulation. In accordance with Article 44(1) of the ESMA Regulation the Board of Supervisors has adopted this opinion.

6. This opinion sets out ESMA's view on how the draft RTS on notifications and the draft RTS on authorisations should be amended in light of the alternative approach set out by the EC in its letters to ESMA.

7. ESMA takes note of the legal interpretation by the EC, limiting the mandates to ESMA in Articles 60(13) and 62(5) of MiCA. However, ESMA also reiterates the importance of the policy objectives pursued by its initial proposals and in particular the need to require a cybersecurity audit realised by a third-party cybersecurity auditor. To ensure that crypto-

[4] https://finance.ec.europa.eu/document/download/52cfebb9-5e13-409f-a970-c613332fffa9_en?filename=240903-letter-esma-mica-crypto-asset-services_en.pdf and https://finance.ec.europa.eu/document/download/72e8db5c-e168-4f4e-9b5a-aaf2f6007ef5_en?filename=240903-letter-esma-mica-crypto-asset-service-provider_en.pdf.

asset service providers are subject to a thorough screening process, including in relation to their ICT systems, prior to their entering into the crypto-assets market, ESMA would thus recommend that the EC amends the level 1 text of the MiCA framework to include such a requirement for a cybersecurity audit realised by a third-party auditor at the time of the authorisation.

3 Background

3.1 Identity and proof of good repute of the members of the management body (Article 7(1) of the draft RTS on authorisations)

8. In relation to the identity and proof of good repute of the members of the management body, the draft RTS on authorisations proposed by the EC depart from the draft RTS submitted by ESMA in March 2024 on several aspects.

Data minimisation in relation to the "personal history" of the members of the management body of the applicant (Article 7(1) of the draft RTS on authorisations submitted by ESMA)

9. The EC suggests amending the first sentence of Article 7(1)(f) of the draft RTS on authorisations to read as follows: "*member's history, namely all the following:*", instead of "*personal history, including all of the following:*" as proposed by ESMA in the final report dated 25 March 2024.

10. In its letter relating to the draft RTS on authorisations, the EC noted that "*In compliance with the principle of data minimisation, the types of information to be collected as part of the "personal history" of the members of the management body of the applicant should be listed exhaustively. Therefore, the first sentence of Article 7(1)(f) of the draft RTS should be drafted so as to ensure that the types information listed thereunder constitute an exhaustive list*".

11. ESMA is of the view that the proposed amendment would resolve concerns raised by the EC while ensuring that essential information for evaluating the "good repute" of members of the management body remains intact. ESMA also believes this amendment would enhance clarity and certainty for applicants regarding the specific information required under Article 62(2)(g) of MiCA.

12. In addition, ESMA understands that such amendment does not preclude national competent authorities from seeking further clarifications relating to the information provided by applicant crypto-asset service providers in relation to the items exhaustively listed in Article 7(1)(f) of the draft RTS on authorisations. As such, the suggested

amendment would not hinder the thorough assessment of the good repute of the members of the management body of applicant crypto-asset service providers by national competent authorities.

Information in relation to criminal records of the members of the management body of the applicant (Article 7(1) of the draft RTS on authorisations submitted by ESMA)

13. For the same reason (data minimisation), the EC suggests limiting the information requested about criminal records to areas "*relevant for the assessment of the authorisation as crypto-asset service provider by bringing the wording of Article 7(1)(f)(i) of the draft RTS on authorisations fully in line with Article 62(3)(a) and (c) of MiCA*".

14. Consequently, Article 7(1)(f)(i) would instead read as follows:

"*(i) proof of clean criminal records;*

*(ii) information on pending criminal proceedings or investigations or penalties (**relating to** commercial law, financial services law, money laundering, and terrorist financing, fraud or professional liability), information on enforcement proceedings or sanctions, information on relevant civil and administrative cases and disciplinary actions, including disqualification as a company director, bankruptcy, insolvency and similar procedures;*" [emphasis added],

instead of the wording initially proposed by ESMA which was:

"*(i) criminal records, including criminal convictions and any ancillary penalties and information on pending criminal proceedings or investigations or penalties (**including relating to** commercial law, financial services law, money laundering, and terrorist financing, fraud or professional liability), information on enforcement proceedings or sanctions, information on relevant civil and administrative cases and disciplinary actions, including disqualification as a company director, bankruptcy, insolvency and similar procedures*," [emphasis added].

15. Article 62(3)(a) of MiCA relating to the assessment of good repute of the members of the management body of the applicant crypto-asset service provider provides that, for all members of its management body, an applicant crypto-asset service provider should provide proof of "*the absence of a criminal record in respect of convictions and **the absence of penalties imposed under the applicable commercial law, insolvency law and financial services law, or in relation to anti-money laundering, and counter-terrorist financing, to fraud or to professional liability***;" [emphasis added].

16. ESMA acknowledges that the amendments suggested by the EC will match the exhaustive list included in Article 62(3)(a) and (c) of MiCA: "*the absence of penalties imposed under the applicable commercial law, insolvency law and financial services law, or in relation to anti-money laundering, and counter-terrorist financing, to fraud or to professional liability".* ESMA takes note of such amendment and does not intend recommending amendments to the EC proposed amendments.

17. However, ESMA wishes to emphasise that the assessment of good repute is of paramount importance in assessing the suitability of members of management bodies in the financial sector and, therefore, in allowing individuals to undertake such roles in entities active in the crypto asset field. Recent experiences in the crypto-assets environment have clearly confirmed the importance of a rigorous assessment of these requirements by supervisors.

18. Consequently, ESMA would recommend to the EC to amend Article 62(3)(a) of MiCA to remove the limitations relating to the scope of the assessment of good repute (in order to include assessment of absence of penalties also in areas other than commercial law, insolvency law, financial services law, anti-money laundering and counter terrorist financing, fraud or professional liability) so that supervisors may carry out a comprehensive assessment of applicants, and of their ability to comply with the relevant requirements of Regulation (EU) 2023/1114.

3.2 ICT systems and related security arrangements (Article 9(b) of the draft RTS on authorisations and Article 4(b) of the draft RTS on notifications)

19. The draft RTS on authorisations (Article 9(b)) and draft RTS on notifications (Article 4(b)) require that applicant crypto-asset service providers submit, as part of their application file, the results of a cybersecurity audit, realised by a third party auditor, with particular reference to Regulation (EU) 2022/2554 on digital operational resilience (DORA). Article 9(b) of the draft RTS on authorisations and Article 4(b) of the draft RTS on notifications stipulate that the cybersecurity audit must cover a minimum of requirements, such as a vulnerability assessment, configuration reviews and penetration tests using different audit approaches/phases (black box, grey box, white box).

20. The EC considers that the above-mentioned provisions create "*a new obligation to conduct an external audit which is not foreseen under DORA and which is not covered by the mandate under MiCA. In addition, this obligation links this cybersecurity audit with the threat-led penetration testing tests (TLPT) which are more specific and regulated under separate provisions under DORA*.".

21. Consequently, the EC suggests to amend Article 9(b) of the draft RTS on authorisations and Article 4(b) of the draft RTS on notifications to provide that "*such a cybersecurity audit, realised by a third party cybersecurity auditor should be provided* ***if available*** *and that the content of a cybersecurity audit should include* ***ideally*** *(but not in a mandatory form) the list included in*" Article 9(b) of the draft RTS on authorisations and Article 4(b) of the draft RTS on notifications.

22. ESMA acknowledges that a restrictive interpretation of the mandates given to ESMA under MiCA (as described in paragraph 1 above) may lead to consider that Article 9(b) of the draft RTS on authorisations and Article 4(b) of the draft RTS on notifications exceed such mandate. Therefore, ESMA takes note of the amendments suggested in the letters of rejection for the draft RTS on authorisation and the draft RTS on notifications and is not recommending amendments to the EC's proposed amendments.

23. However, ESMA wishes to emphasise that technology (in particular, Distributed Ledger Technology) and IT systems are at the core of crypto-asset service providers' activities and that this issue is of paramount importance and raises substantial risk at the authorisation phase, which would be mitigated by performing an external auditor review, to be included in the authorisation or notification material. The absence of these external audits may also lead to fragmentation across the EU, resulting from differences between NCAs and national legal frameworks.

24. Therefore, ESMA would like to urge the EC to amend Articles 60(7) and 62(2) of MiCA to ideally include, in the list of information to be submitted as part of a notification under Article 60 of MiCA or an application under Article 62, a cybersecurity audit, realised by a third-party cybersecurity auditor and meeting minimum requirements similar to those currently detailed in Article 9(b) of the draft RTS on authorisations and Article 4(b) of the draft RTS on notifications. Alternatively, the EC could amend MiCA to give NCAs the possibility to require such cybersecurity audit, where justified with regard to the proportionality principle.