26/02/2025
ESMA75-223375936-6132

Guidelines

On the specification of Union standards for 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 token

Table of Contents

1 Scope

Who?

1. These guidelines apply to competent authorities and to ‘offerors’ as defined in Article 3(1)(13) of MiCA and persons seeking admission to trading of crypto-assets other than asset-referenced tokens or e-money tokens.

What?

2. These guidelines apply in relation to Article 14(1), point (d), of MiCA.

When?

3. These guidelines apply 60 calendar days from the date of their publication on ESMA’s website in all official EU languages.

2 Legislative references, abbreviations and definitions

2.1 Legislative references

ESMA Regulation	Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/77/EC.[1]
MiCA	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.[2]
NIS2 Directive	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.[3]
DORA	Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.[4]

2.2 Abbreviations

EC	European Commission
ESMA	European Securities and Markets Authority
EU	European Union
ART	Asset-referenced token(s)
EMT	E-money token(s)

[1] OJ L 331, 15.12.2010, p. 84.
[2] OJ L 150, 9.6.2023, p. 40.
[3] OJ L 333, 12.12.2022, p. 80–133.
[4] OJ L 333, 14.12.2022, p. 1–79.

2.3 Definitions

network and information system	means 'network and information system' as defined in Article 6, point (1) of NIS2 Directive.
ICT risk	means 'ICT risk' as defined in Article 3, point (5), of DORA.
ICT asset	means 'ICT asset' as defined in Article 3, point (7), of DORA.
access control	means controls to ensure that physical and logical access to ICT assets is authorised and restricted based on business and information security requirements.[5]
offerors and persons seeking admission to trading	refers to the shortened form of 'offerors and persons seeking admission to trading of crypto-assets other than asset-referenced tokens and e-money tokens', for the purposes of these guidelines.

3 Purpose

4. These guidelines, prepared in cooperation with the European Banking Authority, are based on Article 14(1), point (d), of MiCA. The purpose of these guidelines is to specify the appropriate Union standards for offerors and persons seeking admission to trading as regards the maintenance of systems and security access protocols, including policies and procedures. These guidelines also aim to promote greater convergence in the interpretation and application of the MiCA provisions applicable to offerors and persons seeking admission to trading.

[5] *ISO/IEC 29146:2016 Information technology — Security techniques — A framework for access management*. International Organization for Standardization, 2016.

4 Compliance and reporting obligations

4.1 Status of the guidelines

5. In accordance with Article 16 of the ESMA Regulation, competent authorities must make every effort to supervise the implementation of these guidelines and offerors or persons seeking admission to trading should make every effort to comply with them.

6. Competent authorities to which these guidelines apply should incorporate these guidelines into their national legal and/or supervisory frameworks as appropriate, including where particular guidelines are directed primarily at crypto-asset market participants in their jurisdictions. In this case, competent authorities should ensure through their supervision that financial market participants comply with the guidelines.

4.2 Reporting requirements

7. Within two months of the date of publication of the guidelines on ESMA's website in all official EU languages, competent authorities to which these guidelines apply must notify ESMA whether they (i) comply, (ii) do not comply but intend to comply, or (iii) do not comply and do not intend to comply with the guidelines.

8. In case of non-compliance, competent authorities must also notify ESMA within two months of the date of publication of the guidelines on ESMA's website in all official EU languages of their reasons for not complying with the guidelines.

9. A template for notification is available on ESMA's website. Once the template has been filled in, it shall be transmitted to ESMA.

10. Offerors and persons seeking admission to trading are not required to report whether they comply with these guidelines.

5 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

5.1 Guideline 1: General principle on proportionality

11. Offerors and persons seeking admission to trading are expected to make every effort to comply with these guidelines in such a way that is proportionate to, and takes account of, the organisation's size, its overall risk profile, and the nature, scope, and complexity of its activities or operations.

5.2 Guideline 2: Administrative arrangements concerning systems and security access protocols

Administrative arrangements

12. The offeror or person seeking admission to trading should ensure an adequate internal governance and internal control framework is in place for the maintenance of their network and information systems and mitigation of ICT risks. The offeror or person seeking admission to trading should also set clear roles and responsibilities for functions with responsibility for ICT risk management.

13. The offeror or person seeking admission to trading should ensure that the skills of their staff and their budget resources are adequate to support ICT risk management arrangements, with particular reference to those staff responsible for maintenance of network and information systems and access controls, on an ongoing basis. Furthermore, the offeror or person seeking admission to trading should ensure that relevant staff members, including any key function holders, periodically receive appropriate training on ICT risks.

14. The management body of the offeror or person seeking admission to trading should have accountability for setting, approving and overseeing the implementation of the organisation's ICT risk management arrangements, including as it relates to their network and information systems and access controls.

Roles and responsibilities

15. The offeror or person seeking admission to trading should assign to staff within the organisation the responsibility for appropriately identifying, managing, and overseeing ICT risks. It should ensure that the staff in charge of managing ICT risk and security

operations have appropriate arrangements in place to identify, monitor, assess, and report on those ICT risks.

16. The offeror or person seeking admission to trading should ensure that the staff responsible for managing the ICT risks associated with network and information systems and access controls is able to ensure that the identified ICT risks are monitored, assessed, and reported to the management body.

17. The offeror or person seeking admission to trading should define and assign key roles and responsibilities to establish arrangements to:

    i. identify and assess the ICT risks, including those related to ICT services provided by third-party service providers, to which the organisation is exposed;

    ii. define mitigation measures, including controls to mitigate ICT third party risks;

    iii. monitor the effectiveness of the measures referred to in point ii. and take action to correct the measures, where necessary;

    iv. report to the management body on ICT risks and mitigation measures;

    v. identify and assess whether there are any ICT risks resulting from any major change in network and information systems or ICT services (including where provided by third parties), or after any significant operational or security incident;

    vi. manage cryptographic keys through their whole lifecycle.

5.3 Guideline 3: Physical security access protocols

18. Offerors and persons seeking admission to trading should define, document, and implement physical security measures to protect their premises, data centres and sensitive areas from unauthorised access and from environmental hazards. The offeror or person seeking admission to trading should keep a record of each entry to those premises that require authorisation to access.

19. Physical access to network and information systems should be permitted to only authorised individuals according to the need-to-know, least privilege principles and on an ad-hoc basis. Authorisation should be assigned in accordance with the authorised individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be periodically reviewed and withdrawn when no longer required.

20. Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or network and information systems located in these buildings.

5.4 Guideline 4: Security access protocols for network and information systems

21. Logical access to network and information systems should be restricted to authorised individuals designated by the offeror or person seeking admission to trading. Authorisation should be assigned in accordance with the staff's tasks and responsibilities, and limited to individuals who are appropriately trained and whose access to the systems is monitored. Offerors and persons seeking admission to trading should institute controls that reliably restrict such access to network and information systems to those with a legitimate business requirement. Electronic access by applications to data and systems should be limited to the minimum that is required to provide the relevant service.

22. Offerors and persons seeking admission to trading should institute strong controls over privileged system access by strictly limiting and closely supervising staff with elevated system access entitlements. Controls such as role-based access, logging and reviewing of the network and information systems activities of privileged users, strong authentication, and monitoring for anomalies should be implemented. The offeror or person seeking admission to trading should manage access rights to information assets and their supporting systems on a need-to-know and least privilege basis. Logical access rights should be periodically reviewed and withdrawn when no longer required.

23. Access logs should be retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, without prejudice to the retention requirements set out in EU and national law. Offerors and persons seeking admission to trading should use this information to facilitate identification and investigation of anomalous activities that have been detected in the provision of their services.

24. Remote administrative access to critical ICT assets should be granted only on a need-to-know and least privilege basis and only when strong authentication solutions are available.

25. The operation of products, tools and procedures related to access control processes should protect those access control processes from being compromised or circumvented. This includes enrolment, delivery, revocation and withdrawal of corresponding products, tools, and procedures.

5.5 Guideline 5: Cryptographic key management

26. The offeror or person seeking admission to trading should be responsible for cryptographic key management as part of the roles and responsibilities assigned to key staff for ICT risk. These staff of the offeror or persons seeking admission to trading should be responsible for managing cryptographic keys through their whole lifecycle,

including, generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys.

27. Offerors and persons seeking admission to trading should identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure and modification.

28. Offerors and persons seeking admission to trading should develop and implement methods to replace the cryptographic keys in the case of lost, compromised or damaged keys.

29. Offerors and persons seeking admission to trading should create and maintain a register for all certificates and certificate storing devices for at least critical ICT assets. The register should be kept up-to-date.

30. Offerors and persons seeking admission to trading should ensure the prompt renewal of certificates in advance of their expiration.