26/02/2025
ESMA75-223375936-6132

Leitlinien

Über die Spezifizierung der für die Pflege von Systemen und Protokollen zur Gewährleistung der Zugangssicherheit geltenden Standards der Union für Anbieter und Personen, die eine Zulassung zum Handel mit anderen Kryptowerten als vermögenswertereferenzierten Token und E-Geld-Token beantragen

Inhaltsverzeichnis

1 Geltungsbereich

Für wen?

1. Diese Leitlinien finden Anwendung auf zuständige Behörden sowie auf „Anbieter“ (im Sinne der Definition in Artikel 3 Absatz 1 Nummer 13 MiCA) und Personen, die eine Zulassung zum Handel mit anderen Kryptowerten als vermögenswertereferenzierten Token und E-Geld-Token beantragen.

Was?

2. Diese Leitlinien finden Anwendung in Bezug auf Artikel 14 Absatz 1 Buchstabe d MiCA.

Wann?

3. Die Anwendbarkeit dieser Leitlinien beginnt 60 Kalendertage, nachdem diese auf der ESMA-Website in allen EU-Amtssprachen veröffentlicht wurden.

2 Rechtsrahmen, Abkürzungen und Begriffsbestimmungen

2.1 Rechtsrahmen

DORA	Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.[1]
ESMA-Verordnung	Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission.[2]
MiCA	Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937.[3]
NIS-2-Richtlinie	Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148.[4]

[1] ABl. L 333 vom 14.12.2022, S. 1 bis 79.
[2] ABl. L 331, 15.12.2010, S. 84.
[3] ABl. L 150 vom 9.6.2023, S. 40.
[4] ABl. L 333 vom 12.12.2022, S. 80 bis 133.

2.2 Abkürzungen

ART	Asset-referenced token(s), deutsch: vermögenswertereferenzierte(r) Token
EMT	E-money token(s), deutsch: E-Geld-Token
ESMA	Europäische Wertpapier- und Marktaufsichtsbehörde
EU	Europäische Union
Kommission	Europäische Kommission

2.3 Begriffsbestimmungen

Anbieter und Personen, die eine Zulassung zum Handel beantragen	ist die in diesen Leitlinien verwendete Abkürzung für „Anbieter und Personen, die eine Zulassung zum Handel mit anderen Kryptowerten als vermögenswertereferenzierten Token und E-Geld-Token beantragen“.
IKT-Asset	bezeichnet „IKT-Asset“ im Sinne der Definition in Artikel 3 Nummer 7 DORA.
IKT-Risiko	bezeichnet „IKT-Risiko“ im Sinne der Definition in Artikel 3 Nummer 5 DORA.
Netz- und Informationssystem	bezeichnet „Netz- und Informationssystem“ im Sinne der Definition in Artikel 6 Nummer 1 der NIS-2-Richtlinie.
Zugriffskontrolle	bezeichnet auf den Anforderungen an die Geschäfts- und Informationssicherheit beruhende Kontrollen zur Autorisierung und Beschränkung des physischen und logischen Zugangs zu IKT-Assets.[5]

[5] *ISO/IEC 29146:2016 Informationstechnologie – Sicherheitstechniken – Ein Rahmenwerk für die Zugangsverwaltung*. Internationale Organisation für Normung, 2016.

3 Zweck

4. Diese in Zusammenarbeit mit der Europäischen Bankenaufsichtsbehörde erstellten Leitlinien beruhen auf Artikel 14 Absatz 1 Buchstabe d MiCA. Diese Leitlinien bezwecken die Spezifizierung der Standards der Union einschließlich der Strategien und Verfahren in Bezug auf die Pflege von Systemen und Protokollen zur Gewährleistung der Zugangssicherheit, die für Anbieter und Personen, die eine Zulassung zum Handel beantragen, gelten. Darüber hinaus sollen diese Leitlinien größere Konvergenz bezüglich der Auslegung und Anwendung der MiCA-Bestimmungen erzielen, die für Anbieter und Personen, die eine Zulassung zum Handel beantragen, gelten.

4 Einhaltung der Leitlinien und Meldepflichten

4.1 Status dieser Leitlinien

5. Gemäß Artikel 16 der ESMA-Verordnung sind die zuständigen Behörden gehalten, alle erforderlichen Anstrengungen zu unternehmen, um die Umsetzung dieser Leitlinien zu beaufsichtigen, wobei Anbieter oder Personen, die eine Zulassung zum Handel beantragen, alle erforderlichen Anstrengungen unternehmen sollten, diesen Leitlinien nachzukommen.

6. Die diesen Leitlinien unterliegenden zuständigen Behörden sollten diese gegebenenfalls in ihre einzelstaatlichen Rechts- und/oder Aufsichtsrahmen übernehmen; dies gilt auch für jene Leitlinien, die sich in erster Linie an Teilnehmer von Märkten für Kryptowerte in ihren Hoheitsgebieten richten. In diesem Fall sollten die zuständigen Behörden durch ihre Aufsicht dafür Sorge tragen, dass die Finanzmarktteilnehmer diesen Leitlinien nachkommen.

4.2 Mitteilungspflichten

7. Die zuständigen Behörden, für die diese Leitlinien gelten, müssen die ESMA innerhalb von zwei Monaten, nachdem die Leitlinien auf der Website der ESMA in allen Amtssprachen der EU veröffentlicht wurden, darüber unterrichten, ob sie den Leitlinien (i) nachkommen, (ii) nicht nachkommen, jedoch nachzukommen beabsichtigen, oder (iii) nicht nachkommen und nicht nachzukommen beabsichtigen.

8. Zuständige Behörden, die den Leitlinien nicht nachkommen, müssen zudem innerhalb von zwei Monaten ab dem Datum, an welchem die Leitlinien auf der Website der ESMA in allen Amtssprachen der EU veröffentlicht wurden, der ESMA die Gründe für die Nichteinhaltung der Leitlinien mitteilen.

9. Eine entsprechende Vorlage für diese Mitteilung ist auf der ESMA-Website verfügbar. Die ausgefüllte Vorlage ist an die ESMA zu übermitteln.

10. Für Anbieter und Personen, die eine Zulassung zum Handel beantragen besteht keine Pflicht zur Mitteilung, ob sie diesen Leitlinien nachkommen.

5 Leitlinien über die Spezifizierung der für die Pflege von Systemen und Protokollen zur Gewährleistung der Zugangssicherheit geltenden Standards der Union für Anbieter und Personen, die eine Zulassung zum Handel mit anderen Kryptowerten als vermögenswertereferenzierten Token und E-Geld-Token beantragen

5.1 Leitlinie 1: Allgemeiner Verhältnismäßigkeitsgrundsatz

11. Es wird erwartet, dass Anbieter und Personen, die eine Zulassung zum Handel beantragen, alle Anstrengungen unternehmen, diesen Leitlinien in solcher Weise nachzukommen, dass die Größe der Organisation, ihr Gesamtrisikoprofil sowie Art, Umfang und Komplexität ihrer Aktivitäten oder ihres Betriebs berücksichtigt werden und der Verhältnismäßigkeitsgrundsatz gewahrt wird.

5.2 Leitlinie 2: Verwaltungsvereinbarungen in Bezug auf Systeme und Protokolle zur Gewährleistung der Zugangssicherheit

Verwaltungsvereinbarungen

12. Der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sollte eine angemessene interne Unternehmensführung und einen angemessenen internen Kontrollrahmen für die Pflege der eigenen Netz- und Informationssysteme und die Minderung von IKT-Risiken vorsehen. Der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sollte des Weiteren klare Aufgaben und Zuständigkeiten für die Funktionen festlegen, die für das IKT-Risikomanagement verantwortlichsind.

13. Der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sollte sicherstellen, dass die Fähigkeiten ihres Personals – insbesondere der für die Pflege der Netz- und Informationssysteme und der Zugangskontrolle zuständigen Mitarbeitenden – und ihre Budgetmittel angemessen sind, um das IKT-Risikomanagement kontinuierlich zu unterstützen. Des Weiteren sollte der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sicherstellen, dass die relevanten Mitarbeitenden, ggf. einschließlich der Inhaber von Schlüsselfunktionen, in regelmäßigen Abständen geeignete Schulungen über IKT-Risiken erhalten.

14. Das Leitungsorgan des Anbieters oder der Person, die eine Zulassung zum Handel beantragt, sollte für die Festlegung, Genehmigung und Überwachung der Umsetzung der IKT-Risikomanagementmaßnahmen der Organisation rechenschaftspflichtig sein, auch insoweit, als sich dies auf die Netz- und Informationssysteme und Zugangskontrollen bezieht.

Aufgaben und Zuständigkeiten

15. Der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sollte die Verantwortung dafür, dass IKT-Risiken in geeigneter Weise erkannt, gemanagt und überwacht werden, Mitarbeitenden innerhalb der Organisation zuweisen. Dabei ist sicherzustellen, dass das für das Management von IKT-Risiken und Sicherheitsmaßnahmen zuständige Personal geeignete Vorkehrungen für die Erkennung, Überwachung, Bewertung und Berichterstattung über die betreffenden IKT-Risiken getroffen hat.

16. Der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sollte sicherstellen, dass das Personal, das für das Management der IKT-Risiken im Zusammenhang mit Netz- und Informationssystemen und Zugriffskontrollen verantwortlich ist, in der Lage ist, sicherzustellen, dass die erkannten IKT-Risiken überwacht, bewertet und dem Leitungsorgan gemeldet werden.

17. Der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sollte die Schlüsselrollen und -zuständigkeiten festlegen und zuweisen, um Vorkehrungen zu treffen für:

    i. die Erkennung und Bewertung der IKT-Risiken, einschließlich derjenigen, denen die Organisation in Bezug auf von Drittdienstleistern erbrachte IKT-Dienste ausgesetzt ist;

    ii. die Festlegung von Risikominderungsmaßnahmen, einschließlich Kontrollen zur Minderung der IKT-Drittparteienrisiken;

    iii. die Überwachung der Wirksamkeit der in Punkt ii genannten Maßnahmen sowie erforderlichenfalls die Korrektur dieser Maßnahmen;

    iv. die Meldung der IKT-Risiken und Risikominderungsmaßnahmen an das Leitungsorgan;

    v. die Erkennung und Bewertung, ob durch wesentliche Änderungen der Netz- und Informationssysteme oder der IKT-Dienste (auch von Dritten erbrachter IKT-Dienste) oder nach signifikanten betrieblichen oder Sicherheitsvorfällen etwaige IKT-Risiken entstehen;

    vi. das Management kryptografischer Schlüssel während ihres gesamten Lebenszyklus.

5.3 Leitlinie 3: Protokolle für die physische Zugangssicherheit

18. Anbieter und Personen, die eine Zulassung zum Handel beantragen, sollten physische Sicherheitsmaßnahmen festlegen, dokumentieren und umsetzen, um ihre Räumlichkeiten, Datenzentren und sensiblen Bereiche vor unbefugtem Zugang und Umweltgefahren zu schützen. Der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sollte über jeden Zutritt zu den Räumlichkeiten, für die eine Zugangsgenehmigung erforderlich ist, Aufzeichnungen führen.

19. Der physische Zugang zu Netz- und Informationssystemen sollte ausschließlich befugten Personen nach dem Need-to-know-Prinzip, dem Prinzip der minimalen Rechtevergabe und auf Ad-hoc-Basis erteilt werden. Die Befugnis ist entsprechend den Aufgaben und Verantwortlichkeiten der Person, der die Befugnis erteilt wird, zu erteilen und auf Personen zu beschränken, die angemessen geschult sind und überwacht werden. Der physische Zugang ist in regelmäßigen Abständen zu überprüfen und wenn die Befugnis nicht mehr erforderlich ist, ist sie zurückzunehmen.

20. Die angemessenen Maßnahmen zum Schutz vor Umweltgefahren sollten der Wichtigkeit der Gebäude und ihrer Kritikalität für den Betrieb oder die Netz- und Informationssysteme in den betreffenden Gebäuden angemessen sein.

5.4 Leitlinie 4: Protokolle für die Zugangssicherheit für Netz- und Informationssysteme

21. Der logische Zugang zu Netz- und Informationssystemen sollte auf befugte Personen beschränkt sein, die vom Anbieter oder der Person, die eine Zulassung zum Handel beantragt, benannt werden. Die Befugnis ist entsprechend den Aufgaben und Verantwortlichkeiten des Personals zu erteilen und auf Personen, die angemessen geschult sind und deren Zugang zu den Systemen überwacht wird, zu beschränken. Anbieter und Personen, die eine Zulassung zum Handel beantragen, sollten Kontrollen einrichten, die den Zugang zu Netz- und Informationssystemen in zuverlässiger Weise auf diejenigen Personen beschränken, bei denen ein berechtigtes geschäftliches Erfordernis gegeben ist. Der elektronische Zugang von Anwendungen zu Daten und Systemen sollte auf das für die Erbringung des betreffenden Diensts erforderliche Minimum beschränkt sein.

22. Anbieter und Personen, die eine Zulassung zum Handel beantragen, sollten starke Kontrollen für den privilegierten Systemzugang vorsehen, indem sie die Zahl der Mitarbeitenden mit höheren Systemzugangsberechtigungen strikt beschränken und die Mitarbeitenden genauer Aufsicht unterziehen. Es sind Kontrollen zu implementieren, beispielsweise rollenabhängiger Zugang, Protokollierung und Überprüfung der Aktivitäten privilegierter Nutzer in den Netz- und Informationssystemen, starke Authentifizierung sowie Überwachung auf Anomalien. Der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, sollte Zugangsrechte in Bezug auf

Informations-Assets und die dazugehörigen Supportsysteme nach dem Need-to-know-Prinzip und dem Prinzip der minimalen Rechtevergabe erteilen. Die den logischen Zugang gewährenden Rechte sind in regelmäßigen Abständen zu überprüfen und, wenn die Befugnis nicht mehr erforderlich ist, zurückzunehmen.

23. Die Zugangsprotokolle sind so lange aufzubewahren, wie es der Kritikalität der identifizierten Geschäftsfunktionen, den Support-Prozessen und den Informations-Assets angemessen ist; dies lässt die im Unionsrecht und nationalen Recht vorgesehenen Aufbewahrungspflichten unberührt. Anbieter und Personen, die eine Zulassung zum Handel beantragen, sollten diese Informationen dazu nutzen, die Erkennung und Untersuchung im Zuge ihrer Dienstleistungserbringung auftretender anomaler Aktivitäten zu ermöglichen.

24. Der Fernzugang zu kritischen IKT-Assets zu administrativen Zwecken sollte nach dem Need-to-know-Prinzip und dem Prinzip der minimalen Rechtevergabe erteilt werden und auch dann nur, wenn Lösungen für die starke Authentifizierung vorhanden sind.

25. Der Einsatz von Produkten, Tools und Verfahren im Zusammenhang mit Prozessen der Zugangskontrolle sollte die betreffenden Prozesse der Zugangskontrolle davor schützen, kompromittiert oder umgangen zu werden. Dies schließt Anmeldung, Bereitstellung, Widerruf und Rücknahme der entsprechenden Produkte, Tools und Verfahren ein.

5.5 Leitlinie 5: Management kryptografischer Schlüssel

26. Die Verantwortung für das Management der kryptografischen Schlüssel, die als Teil der Aufgaben und Zuständigkeiten für das IKT-Risiko Schlüsselpersonal zugewiesen wird, sollte der Anbieter oder die Person, die eine Zulassung zum Handel beantragt, tragen. Dieses Schlüsselpersonal des Anbieters oder der Person, die eine Zulassung zum Handel beantragt, sollte für die Verwaltung der kryptografischen Schlüssel während ihres gesamten Lebenszyklus verantwortlich sein, wozu u. a. gehört, die Schlüssel zu erzeugen, zu verlängern, zu speichern, zu sichern, zu archivieren, auszulesen, zu übermitteln, außer Dienst zu stellen, zu widerrufen und zu vernichten.

27. Anbieter und Personen, die eine Zulassung zum Handel beantragen, sollten Kontrollen festlegen und umsetzen, um die kryptografischen Schlüssel während ihres gesamten Lebenszyklus vor Verlust, unbefugtem Zugriff, Offenlegung und Veränderung zu schützen.

28. Anbieter und Personen, die eine Zulassung zum Handel beantragen, sollten Methoden für die Ersetzung verlorener, kompromittierter oder beschädigter kryptografischer Schlüssel entwickeln und umsetzen.

29. Anbieter und Personen, die eine Zulassung zum Handel beantragen, sollten zumindest für kritische IKT-Assets ein Register, in dem alle Zertifikate und Zertifikatspeichergeräte verzeichnet sind, anlegen und führen. Das Register ist stets auf dem aktuellen Stand zu halten.

30. Anbieter und Personen, die eine Zulassung zum Handel beantragen, sollten sicherstellen, dass Zertifikate vor ihrem Ablaufdatum erneuert werden.