26/02/2025
ESMA75-223375936-6132

Orientamenti

sulla specificazione delle norme dell'Unione per il mantenimento dei sistemi e dei protocolli di accesso di sicurezza per gli offerenti e le persone che chiedono l'ammissione alla negoziazione di cripto-attività diverse dai token collegati ad attività e dai token di moneta elettronica

Indice

1 Ambito di applicazione

Destinatari

1. I presenti orientamenti si applicano alle autorità competenti e agli «offerenti» di cui all'articolo 3, paragrafo 1, punto 13), del MiCA e alle persone che chiedono l'ammissione alla negoziazione di cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica.

Oggetto

2. I presenti orientamenti si applicano in relazione all'articolo 14, paragrafo 1, lettera d), del MiCA.

Tempistica

3. I presenti orientamenti si applicano a decorrere da 60 giorni di calendario successivi alla loro data di pubblicazione sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE.

2 Riferimenti normativi, abbreviazioni e definizioni

2.1 Riferimenti normativi

Direttiva NIS 2	Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 ([1]).
DORA	Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 ([2]).
MiCA	Regolamento (UE) 2023/1114 del Parlamento europeo e del Consiglio, del 31 maggio 2023, relativo ai mercati delle cripto-attività e che modifica i regolamenti (UE) n. 1093/2010 e (UE) n. 1095/2010 e le direttive 2013/36/UE e (UE) 2019/1937 ([3]).
Regolamento ESMA	Regolamento (UE) n. 1095/2010 del Parlamento europeo e del Consiglio, del 24 novembre 2010, che istituisce l'Autorità europea di vigilanza (Autorità europea degli strumenti finanziari e dei mercati), modifica la decisione n. 716/2009/CE e abroga la decisione 2009/77/CE della Commissione ([4]).

2.2 Abbreviazioni

ART	Token collegati ad attività
CE	Commissione europea
EMT	Token di moneta elettronica
ESMA	Autorità europea degli strumenti finanziari e dei mercati
UE	Unione europea

([1]) GU L 333 del 12.12.2022, pagg. 80-133.
([2]) GU L 333 del 14.12.2022, pagg. 1-79.
([3]) GU L 150 del 9.6.2023, pag. 40.
([4]) GU L 331 del 15.12.2010, pag. 84.

2.3 Definizioni

Controlli di accesso	i controlli volti a garantire che l'accesso fisico e logico alle risorse TIC sia autorizzato e limitato sulla base delle prescrizioni in materia di sicurezza operativa e delle informazioni ([5]).
Offerenti e persone che chiedono l'ammissione alla negoziazione	ai fini dei presenti orientamenti, s'intende la forma abbreviata di «offerenti o persone che chiedono l'ammissione alla negoziazione di cripto-attività diverse dai token collegati ad attività o dai token di moneta elettronica».
Rischi informatici	secondo la definizione di cui all'articolo 3, punto 5), del regolamento DORA.
Risorse TIC	secondo la definizione di cui all'articolo 3, punto 7), del regolamento DORA.
Sistema informativo e di rete	secondo la definizione di cui all'articolo 6, punto 1), della direttiva NIS 2.

3 Finalità

4. I presenti orientamenti, predisposti in collaborazione con l'Autorità bancaria europea (ABE), si basano sull'articolo 14, paragrafo 1, lettera d), del MiCA. Lo scopo dei presenti orientamenti consiste nello specificare le norme dell'Unione appropriate per gli offerenti e le persone che chiedono l'ammissione alla negoziazione per quanto riguarda il mantenimento dei sistemi e dei protocolli di accesso di sicurezza, comprese le politiche e le procedure. I presenti orientamenti mirano inoltre a promuovere una maggiore convergenza nell'interpretazione e nell'applicazione delle disposizioni del MiCA applicabili agli offerenti e alle persone che chiedono l'ammissione alla negoziazione.

([5]) *ISO/CEI 29146:2016 Tecnologie dell'informazione – Tecniche di sicurezza – Quadro di riferimento per la gestione degli accessi*. Organizzazione internazionale per la standardizzazione, 2016.

4 Conformità e obblighi di notifica

4.1 Status degli orientamenti

5. Ai sensi dell'articolo 16 del regolamento ESMA, le autorità competenti devono compiere ogni sforzo per vigilare sull'attuazione dei presenti orientamenti, mentre gli offerenti o le persone che chiedono l'ammissione alla negoziazione dovrebbero compiere ogni sforzo per conformarvisi.

6. Le autorità competenti alle quali si applicano i presenti orientamenti dovrebbero integrarli nei propri quadri giuridici e/o di vigilanza nazionali, a seconda dei casi, anche laddove vi siano orientamenti specifici diretti principalmente ai partecipanti ai mercati di cripto-attività nelle proprie giurisdizioni. In questo caso, le autorità competenti dovrebbero assicurare tramite la propria attività di vigilanza che i partecipanti ai mercati finanziari rispettino gli orientamenti.

4.2 Obblighi di notifica

7. Entro due mesi dalla data di pubblicazione degli orientamenti sul sito web dell'ESMA in tutte le lingue ufficiali dell'UE, le autorità competenti alle quali si applicano i presenti orientamenti devono notificare all'ESMA se i) sono conformi, ii) non sono conformi, ma intendono conformarsi o iii) non sono conformi e non intendono conformarsi agli orientamenti.

8. In caso di non conformità, le autorità competenti devono inoltre notificare all'ESMA, entro due mesi dalla data di pubblicazione degli orientamenti sul sito web dell'Agenzia in tutte le lingue ufficiali dell'UE, i motivi per cui non rispettano tali orientamenti.

9. Sul sito web dell'ESMA è disponibile un modello di notifica. Una volta compilato, siffatto modello deve essere trasmesso all'ESMA.

10. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione non sono tenuti a riferire se sono conformi ai presenti orientamenti.

5 Orientamenti sulla specificazione delle norme dell'Unione per il mantenimento dei sistemi e dei protocolli di accesso di sicurezza per gli offerenti e le persone che chiedono l'ammissione alla negoziazione di cripto-attività diverse dai token collegati ad attività e dai token di moneta elettronica

5.1 Orientamento 1. Principio generale di proporzionalità

11. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero compiere ogni sforzo per conformarsi ai presenti orientamenti in modo proporzionato, tenendo conto delle dimensioni della propria organizzazione, del relativo profilo di rischio complessivo, nonché della natura, della portata e della complessità delle attività o operazioni svolte.

5.2 Orientamento 2. Disposizioni amministrative riguardanti i sistemi e i protocolli di accesso di sicurezza

Disposizioni amministrative

12. L'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe assicurare l'esistenza di una governance e di un quadro di controllo interni adeguati per il mantenimento della propria rete e dei propri sistemi informativi nonché per l'attenuazione dei rischi informatici. L'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe inoltre stabilire ruoli e responsabilità chiari per le funzioni incaricate della gestione dei rischi informatici.

13. L'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe garantire che le competenze del proprio personale e le proprie risorse di bilancio siano adeguate a supportare le disposizioni in materia di gestione dei rischi informatici, con particolare riferimento al personale incaricato del mantenimento della rete e dei sistemi informativi nonché del controllo degli accessi, su base continuativa. Inoltre l'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe assicurare che i membri del personale interessati, compreso il personale che riveste ruoli chiave, ricevano periodicamente una formazione adeguata sui rischi informatici.

14. L'organo di gestione dell'offerente o della persona che chiede l'ammissione alla negoziazione dovrebbe essere responsabile della definizione, dell'approvazione e della supervisione dell'attuazione delle disposizioni in materia di gestione dei rischi informatici dell'organizzazione, anche per quanto riguarda la rete, i sistemi informativi e il controllo degli accessi.

Ruoli e responsabilità

15. L'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe attribuire al personale all'interno dell'organizzazione la responsabilità di individuare, gestire e monitorare adeguatamente i rischi informatici. Dovrebbe altresì assicurare che il personale incaricato della gestione dei rischi informatici e delle operazioni di sicurezza disponga di misure adeguate per individuare, monitorare, valutare e segnalare tali rischi.

16. L'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe garantire che il personale incaricato della gestione dei rischi informatici associati alla rete e ai sistemi informativi nonché al controllo degli accessi sia in grado di assicurare che i rischi informatici individuati siano monitorati, valutati e segnalati all'organo di gestione.

17. L'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe definire e assegnare ruoli e responsabilità chiave per stabilire disposizioni al fine di:

    i. individuare e valutare i rischi informatici, compresi quelli relativi ai servizi TIC erogati da fornitori terzi di servizi, a cui l'organizzazione è esposta;

    ii. definire misure di attenuazione, tra cui controlli per attenuare i rischi informatici derivanti da terzi;

    iii. monitorare l'efficacia delle misure di cui al punto ii. e intervenire per correggere le misure, ove necessario;

    iv. riferire all'organo di gestione in merito ai rischi informatici e alle misure di attenuazione;

    v. individuare e valutare l'esistenza di eventuali rischi informatici derivanti da qualsiasi cambiamento importante nella rete e nei sistemi informativi o nei servizi TIC (anche se forniti da terzi), o dopo qualsiasi incidente operativo o di sicurezza significativo;

    vi. gestire le chiavi crittografiche per tutto il loro ciclo di vita.

5.3 Orientamento 3. Protocolli di accesso di sicurezza fisici

18. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero definire, documentare e attuare misure di sicurezza fisica per proteggere i loro locali, i centri di dati e le aree sensibili dall'accesso non autorizzato e dai rischi ambientali. L'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe tenere un registro di ogni ingresso nei locali per i quali è richiesta un'autorizzazione di accesso.

19. L'accesso fisico alla rete e ai sistemi informativi dovrebbe essere consentito solo alle persone autorizzate in base ai principi della necessità di sapere e del privilegio minimo

e su base ad hoc. L'autorizzazione dovrebbe essere conferita conformemente ai compiti e alle responsabilità della persona autorizzata ed essere limitata a persone opportunamente formate e monitorate. L'accesso fisico dovrebbe essere periodicamente riesaminato e revocato qualora non sia più necessario.

20. Misure adeguate di protezione dai rischi ambientali dovrebbero essere commisurate all'importanza degli edifici e alla criticità delle operazioni o della rete e dei sistemi informativi ubicati in tali edifici.

5.4 Orientamento 4. Protocolli di accesso di sicurezza per la rete e i sistemi informativi

21. L'accesso logico alla rete e ai sistemi informativi dovrebbe essere limitato alle persone fisiche autorizzate designate dall'offerente o dalla persona che chiede l'ammissione alla negoziazione. L'autorizzazione dovrebbe essere conferita conformemente ai compiti e alle responsabilità del personale ed essere limitata a persone opportunamente formate e il cui accesso ai sistemi è monitorato. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero istituire controlli che limitino in modo affidabile l'accesso alla rete e ai sistemi informativi a coloro che hanno un'esigenza operativa legittima. L'accesso elettronico mediante le applicazioni ai dati e ai sistemi dovrebbe essere limitato al minimo necessario per fornire il servizio pertinente.

22. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero istituire controlli rigorosi sull'accesso privilegiato al sistema, limitando in modo stringente e sorvegliando attentamente il personale che dispongono di ampi diritti di accesso al sistema. Dovrebbero essere eseguiti controlli quali l'accesso basato sui ruoli, la registrazione e la revisione delle attività di rete e dei sistemi informativi degli utenti privilegiati, l'autenticazione avanzata e il monitoraggio delle anomalie. L'offerente o la persona chiede l'ammissione alla negoziazione dovrebbe gestire i diritti di accesso alle risorse informatiche e ai relativi sistemi di supporto in base al principio della necessità di sapere e del privilegio minimo. I diritti di accesso logico dovrebbero essere periodicamente riesaminati e revocati qualora non siano più necessari.

23. I registri degli accessi dovrebbero essere conservati per un periodo commisurato alla criticità delle funzioni aziendali, dei processi di supporto e delle risorse informatiche individuati, fatti salvi gli obblighi di conservazione previsti dal diritto dell'UE e nazionale. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero utilizzare queste informazioni per facilitare l'individuazione e l'esame di attività anomale rilevate nella fornitura dei propri servizi.

24. L'accesso amministrativo remoto alle risorse TIC critiche dovrebbe essere concesso solo in base al principio della necessità di sapere e del privilegio minimo e solo quando sono disponibili solide soluzioni di autenticazione.

25. Il funzionamento dei prodotti, degli strumenti e delle procedure relative ai processi di controllo degli accessi dovrebbe proteggere tali processi dalla compromissione o dall'elusione. Ciò include la registrazione, l'erogazione, la revoca e il ritiro dei prodotti, degli strumenti e delle procedure corrispondenti.

5.5 Orientamento 5. Gestione delle chiavi crittografiche

26. L'offerente o la persona che chiede l'ammissione alla negoziazione dovrebbe essere responsabile della gestione delle chiavi crittografiche nell'ambito dei ruoli e delle responsabilità assegnati al personale di riferimento per i rischi informatici. Il personale dell'offerente o delle persone che chiedono l'ammissione alla negoziazione dovrebbe essere responsabile della gestione delle chiavi crittografiche durante il loro intero ciclo di vita, tra cui la generazione, il rinnovo, la conservazione, il backup, l'archiviazione, il recupero, la trasmissione, il ritiro, la revoca e la distruzione delle chiavi.

27. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero individuare e attuare controlli per proteggere le chiavi crittografiche per tutto il loro ciclo di vita dallo smarrimento, dall'accesso, dalla divulgazione e dalla modifica non autorizzati.

28. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero sviluppare e attuare metodi per sostituire le chiavi crittografiche in caso di smarrimento, compromissione o danneggiamento delle stesse.

29. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero creare e tenere un registro per tutti i certificati e i dispositivi di archiviazione dei certificati almeno per le risorse TIC critiche. Il registro dovrebbe essere tenuto aggiornato.

30. Gli offerenti e le persone che chiedono l'ammissione alla negoziazione dovrebbero provvedere al tempestivo rinnovo dei certificati prima della scadenza corrispondente.