Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Draft technical Standards specifying certain requirements in relation to the detection and prevention of market abuse under the Markets in Crypto Assets Regulation (MiCA)

Le titre VI de la réglementation MiCA établit des règles concernant les abus de marché liés à la négociation de crypto-actifs, interdisant les opérations d'initiés, la divulgation illicite d'informations privilégiées et les manipulations de marché, et prévoyant des obligations spécifiques pour la prévention et la détection des comportements abusifs.

Le contenu du rapport de l'ESMA est le suivant :

- Section 2 : Aperçu de la base juridique et du mandat de l'ESMA pour rédiger les RTS.

- Section 3 : Retour d'expérience sur les dispositifs, systèmes et procédures de détection et de prévention des abus de marché.
(Cette section conclut également que le champ d'application des personnes organisant et exécutant des transactions à titre professionnel (PPAET) en vertu de l'article 92 de la MiCA ne sera pas défini dans les RTS. Elle explique également que l'ESMA poursuivra la collecte de preuves et se coordonnera avec la Commission européenne pour obtenir des orientations supplémentaires).

- Section 4 : Modèle de notification pour le signalement de suspicions d'abus de marché (STOR). Il comprend des champs pour l'identification de l'entité déclarante, la description du comportement suspecté, l'identification de la personne suspectée et la fourniture de documents supplémentaires.

- Section 5 : Procédures de coordination pour la détection et la sanction des abus de marché transfrontaliers. Elle établit des protocoles pour l'échange de STOR et d'informations entre les autorités compétentes afin de traiter les cas transfrontaliers.

Quatre annexes :
Annexe I : Analyse coûts/bénéfices réalisée en relation avec le projet de RTS.
Annexe II : Commentaires détaillés des répondants.
Annexe III : Avis reçu par l'ESMA du groupe des parties prenantes du secteur des valeurs mobilières et des marchés (SMSG).
Annexe IV : Projet de texte de RTS.

--> Prochaines étapes : Le projet de RTS a été soumis à la Commission européenne qui décidera de son adoption dans un délai de trois mois, conformément à l'article 10 du règlement (UE) n° 1095/2010.

Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Principaux éléments des RTS

Le champ d'application des obligations en matière d'abus de marché s'applique aux PPAET, y compris les fournisseurs de services de crypto-actifs (CASP) impliqués dans la négociation, la gestion de portefeuille et les services d'échange. Les mineurs, les validateurs, les chercheurs et les constructeurs ne sont pas considérés comme des PPAET aux fins de ces obligations.
Les entités telles que les CASP qui fournissent uniquement des services de conservation ou d'administration sans surveillance transactionnelle ne sont généralement pas considérées comme des PPAET, bien qu'elles fassent l'objet d'une évaluation au cas par cas.

En ce qui concerne les dispositions, les systèmes et les procédures, les PPAET doivent mettre en œuvre des systèmes de surveillance efficaces adaptés à la taille et à l'échelle de leur entreprise, ainsi qu'à la nature de l'activité. Il s'agit notamment d'outils automatisés capables d'effectuer des analyses en temps réel, de superviser les transactions algorithmiques et de surveiller les transactions sur la chaîne et hors chaîne en rapport avec leurs activités.

Les STOR (rapports sur les transactions et les ordres suspects) doivent contenir des informations détaillées sur l'abus présumé, telles que les détails de la transaction, les parties impliquées et les preuves à l'appui des soupçons. Les modèles fournis sont standardisés et adaptés aux spécificités des crypto-actifs, tels que les identifiants de la technologie du grand livre distribué (DLT). Les STOR doivent être soumises aux autorités compétentes sans délai dès qu'un soupçon raisonnable est formé.

Les RTS établissent également des procédures permettant aux autorités nationales compétentes (ANC) de partager les STOR et de coordonner les enquêtes afin de faciliter l'application transfrontalière de la loi.

Éléments de mise en œuvre

(Voir page suivante -->)

Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Éléments de mise en œuvre

La surveillance et la détection doivent être mises en œuvre au moyen de systèmes de surveillance continue des transactions, avec des alertes automatisées en cas d'abus potentiel.
Cette surveillance comprend un examen humain des alertes afin de réduire le nombre de faux positifs et de garantir des rapports exploitables. Les activités de négociation et les aspects DLT sous-jacents (tels que les mécanismes de consensus, lorsqu'ils sont pertinents pour les transactions) doivent être surveillés.

En ce qui concerne le cadre de signalement, le modèle STOR fourni par l'ESMA doit être utilisé pour signaler les abus présumés. Les champs obligatoires tels que les identifiants de transaction, les comportements suspectés ainsi que les documents justificatifs et les informations supplémentaires telles que les adresses des portefeuilles et les hachages de transaction, lorsqu'ils sont disponibles, doivent être inclus dans le STOR.

Les systèmes et les contrôles doivent être adaptés à l'échelle des opérations de l'entité afin que les petites entités puissent s'y conformer. L'externalisation vers des prestataires tiers ou des entités du groupe est autorisée pour les tâches de surveillance, tout en maintenant le contrôle et l'expertise en interne.
Une formation régulière du personnel à la détection des abus de marché est également requise.

Les PPAET doivent documenter les raisons pour lesquelles ils ne soumettent pas de STOR lorsque des alertes sont générées mais jugées non suspectes.
Les systèmes et les procédures doivent être évalués et mis à jour au moins une fois par an et la documentation des changements et des mises à jour des systèmes est requise.

L'ESMA établit également des canaux clairs pour l'échange d'informations entre les ANC, y compris des calendriers et des protocoles de partage de données. L'objectif est de s'assurer que l'ESMA est informée des principaux cas transfrontaliers et, si nécessaire, aide à la coordination.

Les RTS prévoient également une approche neutre sur le plan technologique. Les systèmes doivent tenir compte de l'évolution des technologies telles que l'intelligence artificielle (IA) et l'apprentissage automatique. Les procédures doivent rester adaptables aux nouvelles stratégies ou plateformes de négociation.

L'évaluation et la mise à jour régulières des systèmes de surveillance sont censées s'aligner sur les évolutions du marché et les menaces émergentes.

Sources :
https://www.esma.europa.eu/press-news/esma-news/esma-releases-last-policy-documents-get-ready-mica
https://www.esma.europa.eu/document/final-report-draft-technical-standards-specifying-certain-requirements-relation-detection

Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Title VI of MiCA establishes rules regarding market abuse related to trading crypto-assets, prohibiting insider dealing, unlawful disclosure of inside information, and market manipulation and including specific obligations for the prevention and detection of abusive behaviours.

The content of ESMA's report is as follows:

- Section 2: Overview of the legal basis and ESMA's mandate to draft RTS.

- Section 3: Feedback on arrangements, systems, and procedures for detecting and preventing market abuse.
(This section also concludes that the scope of Persons Professionally Arranging and Executing Transactions (PPAETs) under Article 92 of MiCA will not be defined in the RTS. It also explains that ESMA will continue evidence collection and coordinate with the European Commission for additional guidance).

- Section 4: Notification template for reporting suspected market abuse (STORs). It includes fields for identifying the reporting entity, describing the suspected behaviour, identifying the suspected person, and providing additional documentation.

- Section 5: Coordination procedures for detecting and sanctioning cross-border market abuse. It establishes protocols for exchanging STORs and information among competent authorities to address cross-border cases.

Four Annexes:
Annex I: Cost/benefit analysis undertaken in relation to the draft RTS.
Annex II: Detailed feedback received from respondents.
Annex III: Advice received by ESMA from the Securities and Markets Stakeholder Group (SMSG).
Annex IV: Draft text of the RTS.

Next steps: The draft RTS has been submitted to the European Commission who will decide on adoption within three months, as per Article 10 of Regulation (EU) No 1095/2010.

Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Key elements of the RTS

The scope of market abuse obligations applies to PPAETs, including Crypto-Asset Service Providers (CASPs) involved in trading, portfolio management, and exchange services. Miners, validators, searchers and builders are not considered PPAETs for the purpose of these obligations. Entities such as CASPs only providing custody or administration services without transactional oversight are generally not considered PPAETS, although it shall be assessed on a case-by-case basis.

In relation with arrangements, systems, and procedures, PPAETs must implement effective monitoring systems tailored to their business size and scale, as well as the nature of the activity. It includes automated tools capable of real-time analysis, algorithmic trading oversight, and monitoring both on-chain and off-chain transactions relevant to their operations.

STORs (Suspicious Transaction and Order Reports) must include detailed information about the suspected abuse, such as transaction details, involved parties, and evidence supporting suspicion. The templates provided are standardised and adapted for crypto-asset specifics, such as Distributed Ledger Technology (DLT) identifiers. STORs must be submitted to competent authorities without delay once reasonable suspicion is formed.

The RTS also establish procedures for National Competent Authorities (NCAs) to share STORs and coordinate investigations in order to facilitate cross-border enforcement.

Elements for implementation

Monitoring and detection must be implemented through systems for continuous transaction surveillance with automated alerts for potential abuse. This monitoring includes human review of alerts to reduce false positives and ensure actionable reporting. Both trading activities and underlying DLT aspects (such as consensus mechanisms, when relevant to transactions) must be monitored.

For the reporting framework, the STOR template provided by ESMA shall be used to report suspected abuse. Mandatory fields such as transaction identifiers, suspected behaviours as well as supporting documentation and additional information such as wallet addresses and transaction hashes, when available, have to be included in the STOR.

Systems and controls must be adapted in relation to the scale of the entity's operations to ensure that smaller entities can comply. Outsourcing to third-party providers or group entities is allowed for surveillance tasks while maintaining oversight and expertise in-house. Regular staff training on market abuse detection is also required.

Detailed records of suspicious activities and analyses must be maintained for at least five years.PPAETs should document rationales not submitting STORs when alerts are generated but deemed non-suspicious.

Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA (17 December 2024)

Key elements of the RTS

Systems and procedures must be assessed and updated at least annually and documentation of changes and updates to systems is required.

ESMA also establishes clear channels for exchanging information between NCAs, including timelines and data-sharing protocols. The aim is to ensure that ESMA is informed of major cross-border cases and, when needed, assists in coordination.

The RTS also include a technology-neutral approach. Systems must account for evolving technologies such as Artificial Intelligence (AI) and machine learning. Procedures are expected to be kept adaptable to new trading strategies or platforms.

Regularly assessing and updating monitoring systems is expected to align with market developments and emerging threats.

Sources:
https://www.esma.europa.eu/press-news/esma-news/esma-releases-last-policy-documents-get-ready-mica

https://www.esma.europa.eu/document/final-report-draft-technical-standards-specifying-certain-requirements-relation-detection

Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA
European Securities and Markets Authority

ANNEX

STOR template

Please note that all fields in Sections 1-4 are mandatory. Where information cannot be provided for a specific field, please indicate "NA" and briefly explain the reasons thereof. SECTION 1 — IDENTITY OF ENTITY/PERSON SUBMITTING THE STOR Persons professionally arranging or executing transactions in crypto assets — Specify in each case:	
Name of the natural person	[First name(s) and surname(s) of the natural person in charge of the submission of the STOR within the submitting entity.]
Position within the reporting entity	[Position of the natural person in charge of the submission of the STOR within the submitting entity.]
Name of the reporting entity	[Full name of the reporting entity, including for legal persons: — the legal form as provided for in the register of the country pursuant to the law of which it is incorporated, where applicable, and — the Legal Entity Identifier (LEI) code in accordance with ISO 17442 LEI code.]
Address of the reporting entity	[Full address (e.g. street, street number, postal code, city, state/province) and country.]
Acting capacity of entity with respect to the orders, transactions or behaviours related to the functioning of the distributed ledger technology that could constitute market abuse	[Description of the capacity in which the reporting entity was acting with regards to the order(s), transaction(s) or behaviour(s) related to the functioning of the distributed ledger technology that could indicate the existence of market abuse, e.g. executing orders on behalf of clients, operating a trading platform...]
Type of trading activity (market making, arbitrage etc.) and type of crypto-asset traded by the reporting entity	[Description of any corporate, contractual or organisational arrangements or circumstances or relationships.]

ESMA
European Securities and Markets Authority

Contact for additional request for information	[Person to be contacted within the reporting entity for additional request for information relating to this report (e.g. compliance officer) and relevant contact details: — first name(s) and surname(s), — position of the contact person within the reporting entity, — professional e-mail address, — professional phone number.]
Have the facts already been reported to public authorities?	Please state whether the facts have already been reported to public authority (and in that case indicate the name of the authority).
SECTION 2 — TRANSACTION/ORDER/BEHAVIOUR AND OTHER ASPECTS RELATED TO THE FUNCTIONING OF THE DISTRIBUTED LEDGER TECHNOLOGY	
Description of the crypto-asset:	Describe the crypto-asset(s) which is the subject of the STOR, specifying: — the full name (including Digital Token Identifier (DTI) in accordance with ISO 24165-2 or an equivalent unique identifier as referred to in Article 15 of Commission Delegated Regulation (EU) XXXX/XX (RTS on record-keeping) specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken) or description of the crypto-asset in the absence of DTI. If the suspicious behaviour involves a trading pair, please list both crypto-assets in the pair, — the type of crypto-asset (asset-referenced token (ART), e-money token (EMT), other crypto-asset) and for ARTs and EMTs, the value, right or official currency (or combination thereof) which the crypto-asset references in order to maintain a stable value.
Name(s) of the distributed ledger(s):	[Provide the full name(s) of the distributed ledger(s) where the suspicious behaviour was observed]
Trading platform where order was placed or the transaction was executed	[Specify name and Market Identifier Code (MIC) in accordance with ISO 10383 to identify the trading platform where the order was placed or the transaction was executed.

ESMA
European Securities and Markets Authority

	If the order/transaction was not identified in a trading platform, please mention 'outside a trading platform' and the LEI of the CASP(s) that carried out the transaction if applicable.]
Location (country)	[Full name of the country and the ISO 3166-1 two-character country code.] [Specify: — where the order is given — where the order is executed, — where the behaviour related to functioning of the distributed ledger technology takes place.]
Description of the order, transaction or suspicious behaviour related to the functioning of the distributed ledger technology	[Describe at least the following characteristics of the order(s) transaction(s) or behaviour(s) reported — date(s) and time(s) of the order(s), transaction(s) or behaviour(s). (Dates and times should be reported in UTC per the format in ISO 8601). — transaction reference number or order reference number or transaction hash. — settlement date and time, — purchase price/sale price, — volume/quantity of crypto-assets, — for orders only, the type of order (e.g. 'buy with limit EUR x'), [Where there are multiple orders or transactions that could constitute market abuse the details on the prices and volumes of such orders and transactions can be provided to the competent authority in an Annex to the STOR.] — Information on the order cancellation or alteration including: — the nature of the alteration (e.g. change in price or quantity) and the extent of the alteration,

ESMA
European Securities and Markets Authority

	[Where there are multiple orders or transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, the details on the prices and volumes of such orders and transactions can be provided to the competent authority in an Annex to the STOR.] — the means to alter the order (e.g. via e-mail, phone, etc.). In case of reporting a suspicious behaviour related to the functioning of the distributed ledger, please provide as much detail as possible, including the impact it had on the validation of transactions and the method used to alter the functioning of the distributed ledger.
SECTION 3 — DESCRIPTION OF THE NATURE OF THE SUSPICION	
Nature of the suspicion	[Specify the type of breach the reported order(s), transaction(s), behaviour(s) related to the functioning of the distributed ledger functioning, could constitute market abuse].
Reasons for the suspicion	[Description of the activity (transactions and orders, way of placing the orders or executing the transaction and characteristics of the orders and transactions that make them suspicious, behaviours related to the functioning of the distributed ledger functioning) and how the matter came to the attention of the reporting person and specify the reasons for suspicion. For crypto-assets admitted to trading on/traded on a trading platform, a description of the nature of the order book interaction/transactions that could constitute market abuse.]
SECTION 4 — IDENTIFICATION OF PERSON(S) RESPONSIBLE FOR THE ORDERS, TRANSACTIONS OR BEHAVIOUR RELATED TO THE FUNCTIONING OF THE DISTRIBUTED LEDGER TECHNOLOGY THAT COULD CONSTITUTE MARKET ABUSE ('SUSPECTED PERSON')	
Name	[For natural persons: the first name(s) and the last name(s).] [For legal persons: full name including legal form as provided for in the register of the country pursuant to the

ESMA
European Securities and Markets Authority

	laws of which it is incorporated, if applicable, and Legal Entity Identifier (LEI) code in accordance with ISO 17442.]
National Identification Number	[Number and/or text]. [If the National Identification Number is not applicable or known, provide a date of birth (for natural persons only) in the ISO 8601 format]
Address	[Full address (e.g. street, street number, postal code, city, state/province) and country.]
Information about the employment: — Place — Position	[Information about the employment of the suspected person, from information sources available internally to the reporting entity (e.g. account documentation in case of clients, staff information system in case of an employee of the reporting entity).]
Account number(s) and wallet address(es)	[Numbers of the cash account(s), any joint accounts or any Powers of Attorney on the account the suspected entity/person holds. Wallet address(es) involved in the transaction or suspected behaviour]
Client identifier	[In case the suspected person is a client of the reporting entity.]
Relationship with the issuer of the crypto-asset concerned	[Description of any corporate, contractual or organisational arrangements or circumstances or relationships]
SECTION 5 — ADDITIONAL INFORMATION Background or any other information considered by the reporting entity relevant to the report	
[The following list is indicative and not exhaustive. Other information deemed useful by the reporting person may be provided where relevant to the STOR.] — The position of the suspected person (e.g. retail client, institutions), — The nature of the suspected entity's/person's intervention (on own account, on behalf of a client, validator of transactions in a distributed ledger system, other).	

Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA
European Securities and Markets Authority

— Where the suspected behaviour is conducted on a DLT, other relevant information may include: — whether the transaction passed through a public or private (encrypted) queue of transactions (i.e. mempool) before it was validated on the DLT; — whether the DLT is public (permissionless) or private (permissioned); — potential interactions with smart contracts, for instance specification of the contract address and the function called; — The size of the suspected entity's/person's portfolio, — The date on which the business relationship with the client started if the suspected entity/person is a client of the reporting person/entity, — The type of activity of the trading desk, if available, of the suspected entity, — Trading patterns of the suspected entity/person. For guidance, the following are examples of information that may be useful: — trading habits of the suspected entity/person, — comparability of the size of the reported order/transaction with the average size of the orders submitted/transactions carried out by the suspected entity/person for the past 12 months, — habits of the suspected entity/person in terms of crypto-assets it has traded for the past 12 months, in particular whether the reported order/transaction relates to a crypto-asset which has been traded by the suspected entity/person for the past year. — Other entities/persons known to be involved in the orders or transactions of which could constitute market abuse: — Names, — Activity (e.g. executing orders on behalf of clients, dealing on own account, operating a trading platform, validating transactions.)]
SECTION 6 — DOCUMENTATION ATTACHED
[List the supporting attachments and material together provided with this STOR]. Examples of such documentation are e-mails, recordings of conversations, order/transaction records, distributed ledger technology records, confirmations, broker reports, Powers of Attorney documents, and comment by media where relevant.

Seqlense

RTS – Detection and prevention of market abuse under MiCA

Cécile Henry
General Manager, CLR & Co-Founder

ESMA
European Securities and Markets Authority

Where the detailed information about the orders/transactions/behaviours related to the functioning of the distributed ledger technology referred to in Section 2 of this template is provided in a separate annex, indicate the title of that annex.]