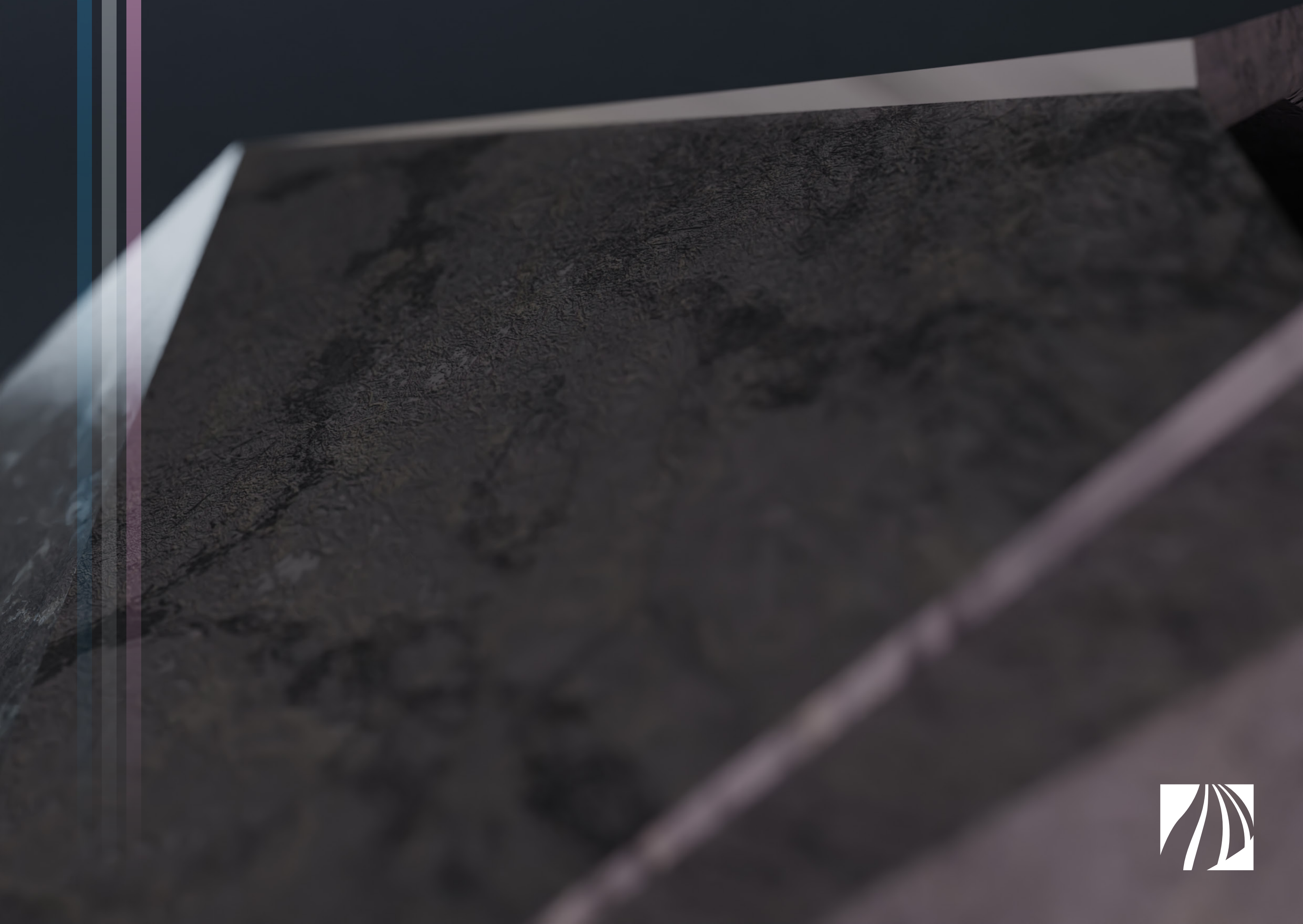
FEBRUARY 2024

REGCOUNSEL FINANCIAL SERVICES WHITE PAPER SERIES #2

Crypto-Asset Service Providers – Authorisation requirements under MiCAR



ABOUT THE AUTHORS

Mr. dr. drs. Jan Jans is a Dutch qualified lawyer specialized in financial regulatory law. He has a strong focus on the regulatory framework covering investment firms, banks, insurance companies, payment service providers, crypto-asset service providers and investment funds. Prior to joining Regulatory Counsel | Financial Services as Partner in 2022, Jan worked as a financial regulatory lawyer at various (international) law firms in the Netherlands.

Jan graduated from Nijmegen University in 2008. In addition to law, he studied financial economics and business administration. He completed the post-academic education Securities Law at the Grotius Academy in 2012. Jan publishes regularly in national law journals and successfully defended his PhD thesis on the level playing field between banks and non-banks in the European market for electronic payments in 2023

✉ jan.jans@recofise.eu ☎ +31 6 83 50 49 27

Mr. drs. Jan-Jouke van der Meer is a Dutch qualified lawyer specialized in financial regulatory law. He advises clients on a broad range of Dutch and EU financial regulatory laws (including MiFID II, MiCAR, PSD2 and AIFMD), licensing issues, corporate governance (including integrity and suitability assessments), compliance and integrity-related issues (including AML and sanctions) and dealing with financial regulators. Prior to joining Regulatory Counsel | Financial Services as Managing Associate, Jan-Jouke worked as a financial regulatory lawyer at an international law firm in the Netherlands.

Jan-Jouke obtained a master's degree (LLM) in Corporate Law from VU Amsterdam in 2018, and holds a master's degree (MSc) in Financial Economics from Erasmus University Rotterdam (2018). He has also published various articles in the area of financial regulatory law.

✉ janjouke.vandermeer@recofise.eu ☎ +31 6 13 50 73 91

Mr. Maarten Mol-Huging is a Dutch qualified lawyer specialised in financial regulatory law. He advises on financial regulatory issues with regards to banks, investment firms, insurers, payment service providers and FinTech (e.g., digital asset services providers), with a particular focus on prudential aspects.

Maarten graduated cum laude at the VU Amsterdam in International Business Law (LLM) in 2022 on his thesis titled: The Biggest Challenge yet for EU Mortgage Lending: The Onset of Artificial Intelligence Tooling. He furthermore completed the prudentially oriented EBI master in EU Banking and Financial Regulation (LLM) at the Frankfurt School of Finance and Management in 2024, writing his thesis on the (civil law) legal position of CET1 capital holders.

✉ maarten.mol-huging@recofise.eu ☎ +31 6 29 90 96 29

Recofise is a boutique law firm located in Amsterdam and specialises in financial regulation. Our clientele consists of financial undertakings (e.g., banks, investment firms and funds, insurance companies, electronic money institutions, payment institutions and crypto-asset service providers) that are active on the Dutch and international financial markets. Recofise has extensive experience in advising and supporting clients with complex legal issues regarding prudential requirements, compliance, risk management, supervisory reporting and supervisory audits.

EXECUTIVE SUMMARY

Within the financial markets, crypto-assets provide for one of the main applications of distributed ledger technology and have therefore become increasingly relevant from a financial regulatory law perspective. Given the unclear regulatory status of crypto-assets and the recent developments in the digital assets market, such as the large increase in market capitalisation of crypto-assets and the negative implications of the failures of Celsius, Voyager and FTX for consumers and other investors, the European Commission stressed the need for having a European legislative framework on crypto-assets that: (i) ensures that Europe will benefit from its opportunities; and (ii) addresses the new risks imposed by this sector.

Given the international and decentralised nature of the market for crypto-assets, it has been crucial that the European legislature adopted MiCAR as an EU Regulation that provides for maximum harmonisation, thereby safeguarding the level-playing field between CASPs as well as the interests of the CASPs' clients in the different EU Member States.

MiCAR is a Regulation that governs: (i) transparency aspects surrounding the issuance and public offering of crypto-assets that are not classified as products or services already regulated by existing European financial law, such as financial instruments under the MiFID II; and (ii) the provision of crypto-asset services by professional parties including financial undertakings.

This White Paper provides a concise overview of the authorisation requirements and processes for businesses that wish to offer crypto-asset services under the MiCAR regime as a CASP or regulated financial undertaking. In general, MiCAR imposes governance, organisational and prudential requirements on CASPs that are to a certain extent akin to those applicable to traditional intermediaries, as well as specific behavioural obligations *vis-à-vis* their customers. Additional requirements are in place for the provision of specific services, such as the custody and administration of crypto-assets on behalf of third parties or the operation of crypto-asset trading platforms.

Different authorisation requirements apply to entities that are already licensed to be active on the financial markets (e.g., banks and investment firms), which only have to follow a notification regime, and new entities that specifically seek authorisation under MiCAR as a CASP. It must be noted that, if a CASP were to engage in certain business operations that qualify as the provision of another regulated service (e.g., a payment service within the meaning of PSD2), the CASP will also have to be authorised in accordance with the regime applicable to that service.

At the moment, ESMA is developing draft RTS that provide further detail regarding the authorisation requirements under MiCAR. Although these level 2 regulations have not yet been finalised, the draft RTS provide a valuable insight as to how CASPs will be required to structure their business and compliance environment, making them inexorable to any MiCAR preparation. As CASPs have, in principle, until 30 December 2024 to complete the authorisation process, which shall open in the Netherlands in the course of Q2 2024, it is essential for market participants to already commence their preparations for an application or notification if they intend to start offering crypto-asset services as of 30 December 2024.

TABLE OF CONTENTS

1. INTRODUCTION

1. INTRODUCTION

This White Paper covers an in-depth review of the authorisation requirements applicable to Crypto-Asset Service Providers (“**CASPs**”) under the Markets in Crypto-Assets Regulation (“**MiCAR**”).[1] As MiCAR already entered into force and will, largely, apply from 30 December 2024, compliance with its extensive requirements becomes more and more topical. Moreover, the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten,* “**AFM**”) and the European Securities and Markets Authority (“**ESMA**”) recently called upon market participants to start preparing their organisations for the application of MiCAR, even *in lieu* of concrete authorisation regimes. The AFM recently indicated that it will likely open the application procedure in April or May 2024.[2]

Since the entering into force of MiCAR, ESMA has published two (2) packages of draft technical standards, in June[3] and October 2023,[4] which both contain detailed rules refining the broad provisions of MiCAR. The third and final package of draft technical standards is expected to be published in Q1 2024, with the first elements of this package already published at the time of writing.[5] Whilst the technical standards of the published packages remain drafts at the moment, it is necessary to carefully consider its norms and provisions, as, in preparing for an authorisation application, firms cannot properly act without taking due notice of these details. In this sense, it is necessary for market participants to take preparatory action on the basis of documentation that may still be subject to change in order to meet the implementation deadline of 30 December 2024.

In this White Paper, we set out the framework applicable to a CASP authorisation, referencing, where possible, relevant (draft) legislation. In course of doing so, we also compare the regime applicable to CASPs under MiCAR with the regime applicable to investment firms under the Markets in Financial Instruments Directive II (“**MiFID II**”).[6] That being said, this White Paper does not intend to provide an all-encompassing comparative assessment of the two, and any references to MiFID II are solely included for comparability purposes and aim to give an element of recognisability to the sometimes abstract provisions of MiCAR.[7]

[1] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

[2] As indicated by the AFM during a seminar regarding CASP applications held on 25 January 2024.

[3] ESMA, Consultation Paper: Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCAR), (2023), (hereinafter: “**ESMA, 2023a**”).

[4] ESMA, Consultation Paper: Technical Standards specifying certain requirements of Markets in Crypto Assets Regulation (MiCAR) - second consultation paper, (2023), (hereinafter: “**ESMA, 2023b**”).

[5] Being the ESMA Consultation Paper on the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments, (2024); and the ESMA Consultation Paper on the draft guidelines on reverse solicitation under the Markets in Crypto Assets Regulation (MiCA), (2024).

[6] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

[7] As the delegated regulations pertaining to MiCAR are yet to be adopted, and the majority even published, useful guidance can be found in the existing level 2 MiFID II texts or PSD2 texts which could provide more concrete requirements than may be deduced from the abstract level 1 Regulation.

This White Paper also does not deal with: (i) the qualification of so-called asset-referenced tokens ("**ARTs**") or e-money tokens; and (ii) the transparency regime surrounding the issuance of crypto-assets.

It must be borne in mind that, fundamentally, MiCAR does not purport to be the distributed ledger technology ("**DLT**") based equivalent of MiFID II. Supervisory authorities have time and again warned that MiCAR will provide a substantially lower level of protection to the customer, whereby not all significant risks of crypto-assets can be excluded. Principally, MiCAR still adheres to the principle of *technological neutrality*, i.e., the legislative approach whereby it is indifferent to the technological basis of the regulated item.[8] Nevertheless, it becomes clear that in a larger trend of *mifidisation* MiCAR takes a large amount of inspiration from the regulatory framework applicable to dealings in financial instruments.

This White Paper is specifically addressed to those parties that:

I currently offer crypto-asset services (as defined in MiCAR) and wish to continue to do so upon the applicability of MiCAR, whether or not by relying on the "grandfathering" regime of art. 143(3) MiCAR;

II seek to first offer crypto-asset services upon the applicability of MiCAR; and

III do not become subject to an authorisation requirement as a CASP, but still wish to know what services they can provide upon the applicability of MiCAR without requiring a CASP authorisation.

[8] See for example Art. 4(15) MiFID II; which was strikingly amended by the DLT Pilot Regime Regulation to include the wording '... including such instruments issued by means of distributed ledger technology' clarifying the applicability of MiFID II to security tokens, thereby technically disproving the principle of technological neutrality. After all, a financial instrument is a financial instrument, fully disregarding the technology it is based upon. Why this is a problematic statement, see (briefly) paragraph 2.

In line with the recommendations of ESMA and the AFM, we identify the following steps that can be taken by market participants (including those that are already regulated) that intend to provide, or intend to continue providing, crypto-asset services upon the applicability of MICAR:

I perform an analysis on the extent to which crypto-asset services are provided, and if so, which crypto-asset services are provided and whether a CASP authorisation is required.

II perform a gap-analysis on the extent to which certain existing policies comply with the requirements of MiCAR, for instance those already drafted in accordance with MiFID II or national virtual asset authorisation regimes (e.g., the current national registration regime for virtual asset service providers under the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*, the "**Dutch AML Act**")).

III draft a position paper to be shared with the AFM to obtain confirmation whether the services provided are in scope of MiCAR.

IV specifically for regulated financial undertakings that wish to use the notification regime:

- create a transition plan.
- clarify the regulatory status of products and services already offered and that involve the use of DLT.

Moreover, the AFM has made available a specific *pre-scan* procedure. In the pre-scan procedure, market participants are able to discuss aspects such as scoping and taxonomy, i.e., to what extent a CASP authorisation is required and for which services. We highly recommend parties to make use of this procedure, based on a thoroughly drafted position paper, in order to ensure an as smooth as possible authorisation process. The pre-scan procedure is open as of the date of writing this White Paper.

This White Paper is structured as follows. In Section 2, we address the crypto-asset services that are covered by MiCAR. In Section 3, we cover the various possibilities for providing crypto-asset services (e.g., authorisation). Thereafter, we cover the requirements applicable to fully authorised CASPs, i.e., governance requirements (Section 4), prudential requirements (Section 5), requirements applicable to qualifying holdings (Section 6), safeguarding requirements (Section 7), and record-keeping and reporting requirements (Section 8). In Section 9, we cover the requirements applicable to CASPs authorised under the notification regime.

2. CRYPTO-ASSET SERVICES COVERED BY MICAR

2. CRYPTO-ASSET SERVICES COVERED BY MICAR

MiCAR, in principle, applies to natural and legal persons and *certain other undertakings* that are engaged in the issuance, offer to the public and admission to trading of crypto-assets or that provide services related to crypto-assets in the European Union ("**EU**").[9] MiCAR prohibits a person from providing crypto-asset services, unless that person is either: (i) a legal person or other undertaking that has been authorised as a CASP (i.e., the full authorisation regime); or (ii) a regulated financial undertaking that is allowed to provide crypto-asset services (i.e., the notification regime).[10]

Due to the (often) decentralised nature of the provision of crypto-asset services, MiCAR specifically provides for an authorisation requirement in case such decentralised provision is considered to be controlled by a legal or natural person. The third group of MiCAR subjects are *certain other undertakings*, which constitute a highly interesting and broad category of persons in light of the decentralised crypto-world. If, however, a service is provided on a fully decentralised basis, i.e., without the intermediation of any party, such service is not covered by MiCAR.[11] This exclusion of decentralized finance ("**DeFi**") is exemplary of what has been coined as the great gap of MiCAR, namely the issue of its scope of application, largely reducing to MiCAR's taxonomy issues.[12]

The taxonomy issue relates to the *prima facie* simple scope of MiCAR, which seeks to govern all crypto-assets (issued with DLT or similar technology) that are not already regulated under another Regulation or Directive (e.g., tokens that are financial instruments fall under the scope of MiFID II).[13] This negative frame, i.e., all crypto-assets that are not already regulated otherwise, permits for a very broad scope of application that may interfere with national law doctrines, such as that of the financial product (*financieel product*) under the Dutch Act on Financial Supervision (*Wet op het financieel toezicht*, "**FSA**") or the delineation between MiCAR and collective investment units regulated under the AIFMD[14].[15]

[9] Art. 2 MiCAR.

[10] Art. 59 MiCAR.

[11] Recital (22) MiCAR.

[12] F. Annunziata, An overview of the Markets in Crypto Assets Regulation (MiCAR), 158 EBI Working Paper, (2023).

[13] Art. 2(4) MiCAR; see also the ESMA Consultation Paper on the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments, (2024); wherein ESMA (attempts to) delineates the division between financial instruments and crypto-assets from an EU law perspective.

[14] Directive 2011/61/EU of the European Parliament and of the Council of 8 June 2011 on Alternative Investment Fund Managers (AIFMD).

[15] See for an extensive discussion: D. Zetsche, F. Annunziata and J. Sinnig, Digital Assets, MiCA and EU Investment Fund Law, (2023).

Furthermore, it is equally enigmatic what comprises *similar technologies* or the residual category of crypto-assets other than ARTs or e-money tokens. Similarly, the exclusion of non-fungible tokens ("**NFTs**") from the scope of MiCAR does not make its taxonomy easier, as MiCAR itself recognises that the excluded status of NFTs is dependent on a number of modalities surrounding their issuance.[16]

Although the purpose of this White Paper is not to develop a (Dutch) taxonomy of what is considered to be a crypto-asset in scope of MiCAR, we recommend that any entity wishing to issue a product or service using DLT obtains an assessment of a law firm defining the qualification of such product or service as a crypto-asset within the meaning of MiCAR, i.e., in how far the token in question is a *'digital representation of a value or of a right that is able to be transferred and stored electronically using DLT or similar technology.'*

Such an advice, whether in the form of a legal opinion, memorandum or gap-analysis, is quintessential in identifying the scope of regulatory requirements applicable pursuant to MiCAR. Given the issues with the taxonomy of the crypto-assets covered by MiCAR identified above, we believe that this analysis may be more complicated than it would first seem and ideally comprises a verification with the AFM.

[16] Art. 2(3) and Recital (10) and (11) MiCAR.

Below, we include a list of crypto-asset services that a CASP may be authorised to provide, which list is reminiscent of the investment services under MiFID II. For completeness' sake, we note that the MiFID II-equivalent of the service of "custody and administration of crypto-assets on behalf of clients" only qualifies as an ancillary service *(nevendienst)* under MiFID II, exemplifying the recent developments in the *crypto winter* where large issues with respect the safeguarding of client assets and funds were plentiful, causing the EU legislature to lift this service to a service subject to a full authorisation regime under MiCAR.

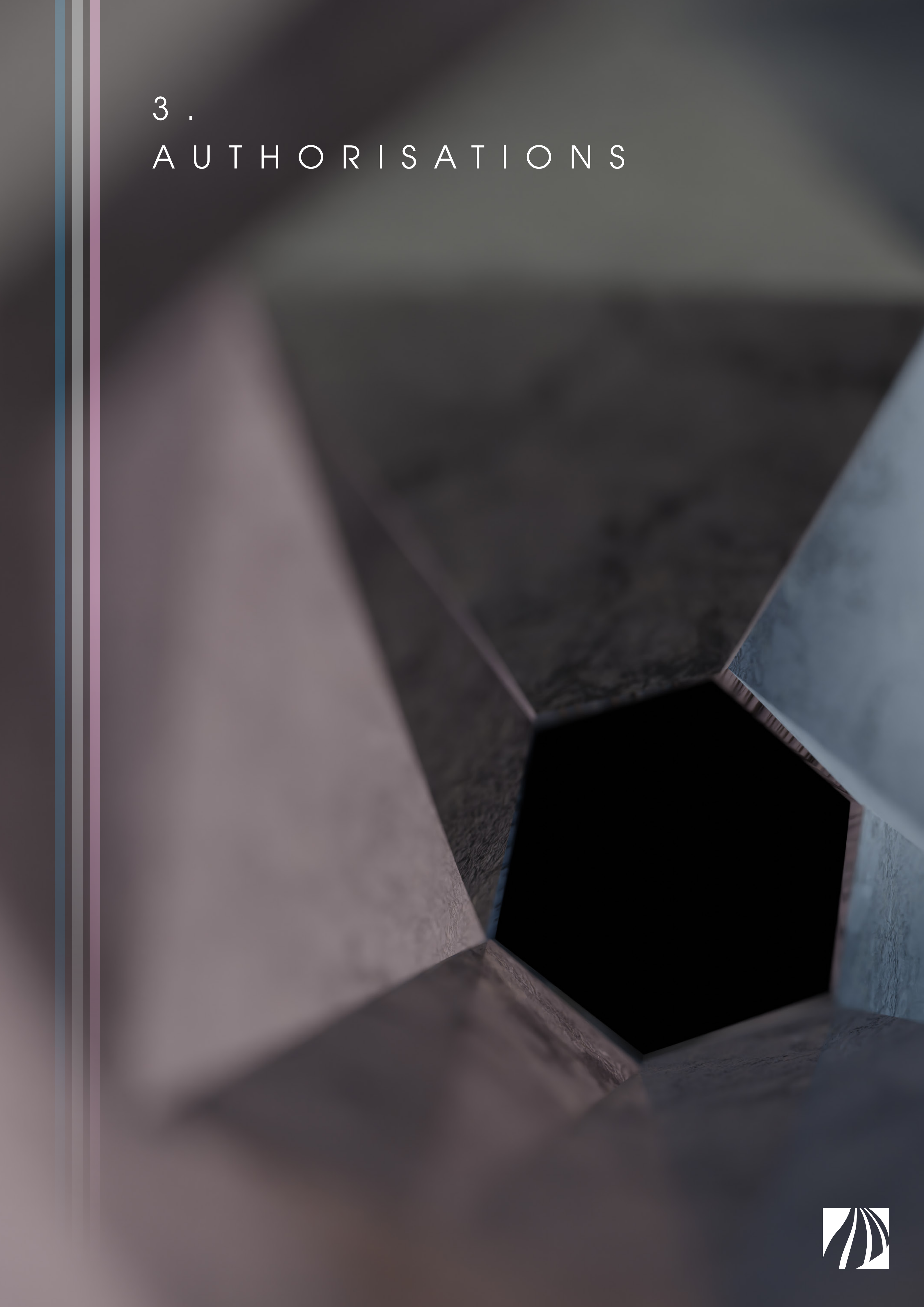
Table 1: MiCAR Crypto-asset services

MiCAR Service	Description	Relevant MiCAR article
Providing custody and administration of crypto-assets on behalf of clients	The safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys	Art. 75
Operation of a trading platform for crypto-assets	The management of one or more multilateral systems, which bring together or facilitate the bringing together of multiple third-party purchasing and selling interests in crypto-assets, in the system and in accordance with its rules, in a way that results in a contract, either by exchanging crypto-assets for funds or by the exchange of crypto-assets for other crypto-assets	Art. 76
Exchange of crypto-assets for funds	The conclusion of purchase or sale contracts concerning crypto assets with clients for funds by using proprietary capital	Art. 77
Exchange of crypto-assets for other crypto-assets	The conclusion of purchase or sale contracts concerning crypto-assets with clients for other crypto-assets by using proprietary capital	Art. 77
Execution of orders for crypto-assets on behalf of clients	The conclusion of agreements, on behalf of clients, to purchase or sell one or more crypto-assets or the subscription on behalf of clients for one or more crypto assets, and includes the conclusion of contracts to sell crypto-assets at the moment of their offer to the public or admission to trading	Art. 78
Placing of crypto-assets	The marketing, on behalf of or for the account of the offeror or a party related to the offeror, of crypto-assets to purchasers	Art. 79
Reception and transmission of orders for crypto-assets on behalf of clients	The reception from a person of an order to purchase or sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution	Art. 80

Providing advice on crypto-assets[17]	Offering, giving or agreeing to give personalised recommendations to a client, either at the client's request or on the initiative of the CASP providing the advice, in respect of one or more transactions relating to crypto-assets, or the use of crypto-asset services	Art. 81
Providing portfolio management of crypto-assets	Managing portfolios in accordance with mandates given by clients on a discretionary client-by-client basis where such portfolios include one or more crypto-assets	Art. 81
Providing transfer services for crypto-assets on behalf of clients	Providing services of transfer, on behalf of a natural or legal person, of crypto-assets from one distributed ledger address or account to another	Art. 82

[17] Art. 81(3) and (5) provide for the ban on inducements equivalent to that of MiFID II, where inducements related to independent investment advice are limited to minor non-monetary benefits and inducements in the course of portfolio management is subject to a complete prohibition. See also Recital (89).

3. AUTHORISATIONS



3. AUTHORISATIONS

3.1 Introduction

In this Section, we explore the regulatory possibilities for persons that wish to provide crypto-asset services in the Netherlands.[18] As the final technical standards on authorisations have yet to be published, we base our assessment on the documentation currently available.[19] At the time of writing of this White Paper, ESMA has, as set out above, issued the first two (2) packages of draft technical standards and is expected to publish the third in Q1 2024.[20] The published ITS and RTS mostly see to the required information for the creation of the authorisation procedures, something ESMA stresses the competent authorities should work on. The AFM has primarily taken up this task in the Netherlands. However, the final delineation between its supervisory scope and that of the Dutch Central Bank *(De Nederlandsche Bank*, "**DNB**") has yet to fully crystallise, albeit that it seems fairly certain in the latest draft Dutch regulation.[21]

MiCAR, broadly speaking, recognises two possible avenues for obtaining supervisory authorisation for the provision of crypto-asset services, being: (i) a full authorisation procedure (Section 3.2); or (ii) a notification procedure (Section 3.3). We note that the latter is only available for certain regulated financial undertakings.

Although this does not serve as the main topic of this White Paper, we note that entities may also be able to provide crypto-asset services in the Netherlands on the basis of: (i) a passport (Section 3.4); (ii) reverse solicitation (Section 3.5); or (iii) an exemption (Section 3.6).

[18] Art. 59 and 62 MiCAR.

[19] AFM, Presentation: MiCAR – AFM Update, (2023).

[20] Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included in an application for authorisation as CASP.

[21] See the Draft implementation decree MiCAR and TFR (*Uitvoeringsbesluit verordening cryptoactiva en verordening bij geldovermakingen en overdrachten van cryptoactiva te voegen informatie*).

3.2 Full authorisation procedure

3.2.1 General

For those entities that wish to provide crypto-asset services upon the applicability of MiCAR (i.e., 30 December 2024) under a full CASP authorisation, the application process under art. 62 MiCAR must, in principle, be completed by 30 December 2024. We note however that MiCAR includes two relevant Member State options in this respect.

First, art. 143(3) MiCAR provides for a so-called "grandfathering" regime, which stipulates that CASPs that provide their services in accordance with applicable law before 30 December 2024 may continue to do so until 1 July 2026 or until they are granted or refused an authorisation, whichever is sooner. Member States may however decide not to apply said transitional regime or to reduce its duration where they consider that their national regulatory framework applicable before 30 December is less strict than MiCAR. In this respect, we note that on 14 July 2023 the Dutch Minister of Finance launched a consultation to seek views on a draft Implementation Act MiCAR (*Uitvoeringswet verordening cryptoactiva*, "**Consultation Act**"). In the draft explanatory notes to the Consultation Act (*Memorie van Toelichting*), the Dutch Minister of Finance stipulates that the Netherlands will apply this Member State option, whereby the intention is, subject to consultation with the AFM and DNB, to reduce the transitional period to a maximum of six (6) months.

In its report on the consultation views (*consultatieverslag*), the Dutch Minister of Finance indicates that several market parties submitted their views on the Consultation Act, of which more than half raised concerns about, *inter alia*, the feasibility of the Member State option regarding shortening the transitional period to a maximum of six (6) months after MiCAR becomes applicable. The Dutch Minister of Finance has however decided not to change anything in this respect, and notes that DNB and the AFM have indicated that a transitional period of six (6) months is feasible from their perspective. This means that, although the Consultation Act has yet to pass the Dutch House of Representatives (*Tweede Kamer*) and the Dutch Senate (*Eerste Kamer*) (meaning that the final text may still be subject to amendments), CASPs that currently provide their services in the Netherlands under the national registration regime of the Dutch AML Act may only continue to do so until 30 June 2025 or until they are granted or refused an authorisation as a CASP under MiCAR, whichever is sooner.[22]

[22] See also Art. 8a of the draft implementation decree MiCAR and TFR (*Uitvoeringsbesluit verordening cryptoactiva en verordening bij geldovermakingen en overdrachten van cryptoactiva te voegen informatie*). This decree went into consultation on 22 January 2024, signaling that the Dutch legislature still intends to maintain the 6 months period.

Secondly, art. 143(6) MiCAR includes a Member State option allowing Member States to apply a simplified procedure for applicants for an authorisation application that is submitted between 30 December 2024 and 1 July 2026 by entities that, on 30 December 2024, were authorised under national law to provide crypto-asset services. The explanatory notes to the Consultation Act stipulate that the Netherlands will not adopt this Member State option, as the Netherlands currently applies a mere registration regime (rather than an authorisation regime).

In general, we note that the authorisation regime under MiCAR resembles the regime applicable to investment firms under MiFID II, with the AFM for now even explicitly referring interested parties to MiFID II documentation *in lieu* of MiCAR specific authorisation documentation. Yet certain (important) differences exist, which will be dealt with in more detail in Section 4 and further.

3.2.2 Timing

As a preliminary indication of a timeline, the AFM guestimates that an application procedure will take approximately five (5) months. However, the AFM notes that, due to circumstances (e.g., amendments to be made by an applicant upon the AFM's request) this period may be longer. Also in view of the submitted views of market parties on the Consultation Act, we consider there to be a possibility that the AFM will be somewhat overwhelmed with the amount of applications, especially so towards the end of 2024.

It is therefore essential for potential applicants to start the introductory talks with the AFM as soon as possible and, preferably, already in the first half of 2024. In this respect, the AFM helpfully facilitates a voluntary pre-scan procedure for parties who are preparing for a CASP authorisation application to contribute to a more efficient formal authorisation procedure and build knowledge on both sides on important topics. In general, the idea of the AFM behind this pre-scan procedure is to have meetings with the AFM to align on the most important topics in an efficient manner. The pre-scan procedure is open at the date of writing this White Paper and the AFM recently indicated that it will likely open the application procedure in April or May 2024.

3.3 Notification procedure

3.3.1 General

As MiCAR presumes that certain financial undertakings would generally be capable of providing crypto-asset services in a controlled manner[23], MiCAR provides for a notification regime for:

I credit institutions that wish to provide crypto-asset services;

II central securities depositories that wish to provide custody and administration of crypto-assets on behalf of clients;

III investment firms that wish to provide crypto-asset services equivalent to the investment services and activities for which it is authorized under MiFID II;

IV electronic money institutions that wish to provide custody and administration of crypto-assets on behalf of clients and transfer services for crypto-assets on behalf of clients with regard to the e-money tokens it issues;

V UCITS management companies or alternative investment fund managers that wish to provide crypto-asset services equivalent to the management of portfolios of investment and non-core services for which they are authorised under the UCITS Directive[24] or the AIFMD; and

VI market operators authorised under MiFID II that wish to operate a trading platform for crypto-assets.

Instead of having to complete a full authorisation procedure, said regulated financial undertakings may rely on their existing documentation which principally only has to be amended slightly to fit the envisaged crypto-asset services.

[23] ESMA, 2023a, paragraph 8.

[24] Directive 2009/65/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS).

Furthermore, data that has already been submitted by the regulated entity to the AFM[25] does not have to be resubmitted, provided that the data remains up-to-date.[26] Therefore, such applicants are most likely relieved from the duty to resubmit corporate data or policies that are not (or only slightly) affected by the new crypto-asset services.[27] Once the AFM confirms that the notification is complete, the financial entity may, provided all information provided is adequate, ensue with crypto-asset service provision.[28]

In Section 9, we set out the specific authorisation requirements that apply to the notification regime.

3.3.2 Interaction between crypto-asset services and other regulated services

Whether regulated financial undertakings can suffice with a notification procedure instead of a full authorisation procedure, thus depends on the type of licence they hold (e.g., an AIFM licence or a credit institution licence) and the corresponding crypto-asset service they wish to provide.[29] In this context, we include below relevant remarks on the interaction between crypto-asset services and other regulated services.

[25] Where the competence of the AFM to receive the notifications, and not the ECB or DNB, is contained in art. 60 MiCAR and confirmed in ESMA Q&A 2089.

[26] Art. 60(9) MiCAR; This is further amplified (potentially) by the fact that notifying financial undertakings are, upon successful reception and no objection to the notification, excepted from Art. 62, 63, 64, 67, 83 and 84 MiCAR.

[27] This is further amplified (potentially) by the fact that notifying financial undertakings are, upon successful reception and no objection to the notification, excepted from articles 62, 63, 64, 67, 83 and 84.

[28] Art. 60(8) MiCAR.

[29] Art. 60 MiCAR.

3.3.2.1 Investment services and activities

Arguably most important for regulated financial undertakings wishing to provide crypto-asset services, MiCAR gives a concordance list for MiFID II services and crypto-asset services, which when transcribed reads as represented below.

Table 2: Concordance table of MiFID II investment services and MiCAR crypto-asset services

MiFID II Annex I	Investment service	Crypto-asset service
Section B (1) (Ancillary)	Safekeeping and administration of financial instruments for the account of clients	Custody and administration of crypto-assets on behalf of clients
Section A (8) and (9) resp.	Operation of a multilateral trading facility ("**MTF**") and operation of an organised trading facility ("**OTF**")	Operation of a trading platform for crypto-assets
Section A (3)	Dealing on own account	Exchange of crypto-assets for funds or other crypto-assets
Section A (2)	Execution of orders on behalf of clients	Execution of orders for crypto-assets on behalf of clients
Section A (6) and (7) resp.	Underwriting or placing of financial instruments on a firm commitment basis and placing of financial instruments without a firm commitment basis	Placing of crypto-assets
Section A (1)	Reception and transmission of orders in relation to one or more financial instruments	Reception and transmission of orders for crypto-assets on behalf of clients
Section A (5)	Investment advice	Providing advice on crypto-assets
Section A (4)	Portfolio management	Providing portfolio management on crypto-assets

A service that in our view should be further clarified by the supervisors is that of the "exchange of crypto-assets for funds or other crypto-assets"[30], and more specifically: (i) whether "traditional" proprietary traders (e.g., market makers) are understood to conduct such activity if they conduct their activities in respect of crypto-assets; and (ii) how this service relates to the service of "execution of orders for crypto-assets on behalf of clients" ("**MiCAR Order Execution**").

[30] I.e., the services of "exchange of crypto-assets for funds" and the "exchange of crypto-assets for other crypto-assets" as referred to under art. 3(1)(16)(d) and (e) MiCAR.

This is especially relevant now that art. 60(3)(c) MiCAR stipulates that investment firms may (under the simplified notification procedure) provide crypto-asset services in the EU equivalent to the investment services and activities for which they are specifically authorised under MiFID II, whereby the "exchange of crypto-assets for funds and other crypto-assets" is deemed equivalent to dealing on own account under Section A, point (3), Annex I MiFID II. Accordingly, if proprietary traders that hold an investment firm licence are understood to conduct the "exchange of crypto-assets for funds or other crypto-assets" in the event that they conduct their activities in respect of crypto-assets, they would need to go through the notification procedure and are subject to certain MiCAR requirements.

Exchanging of crypto-assets for funds or other crypto-assets

Confusingly, art. 3(1)(16) MiCAR defines the crypto-asset service of "exchanging crypto-assets for funds or other crypto-assets" as the "conclusion of purchase or sale contracts concerning crypto-assets **with clients** for other crypto-assets (or funds) by using proprietary capital",[31] where clients (similar as under MiFID II) are those natural or legal persons to whom a CASP provides crypto-asset services. The combination of the definition of the service and that of the "client" comes across as a circular reasoning, i.e., a service qualifies as the regulated activity of exchanging crypto-assets when it is conducted *vis-à-vis* a "client", and a client qualifies as a MiCAR-client when it is provided the regulated service of exchanging crypto-assets. This raises the question as to whether proprietary trading in respect of crypto-assets (e.g., market makers that engage in the continuous offering of buying and selling crypto-assets for own account at self-set prices *vis-à-vis* (professional) counterparties that in no way rely on said market maker to protect its interests) falls under the MiCAR-equivalent of "dealing on own account" (or whether the scope of the MiCAR-equivalent is more narrow).

[31] Art. 3(1)(20) MiCAR.

In the absence of guidance from the supervisory authorities, the following arguments could be made to support the view that proprietary traders are not considered to provide the regulated service of exchanging crypto-assets if they conduct their activities in respect of crypto-assets:

I the definition of "dealing on own account" under MiFID II does not refer to clients, whereas the definition under MiCAR does, suggesting that the scope of the service under MiCAR is more narrow and does not include activities conducted *vis-à-vis* non-clients (e.g., counterparties).

II also in view of the wording of the definition of a "client" under MiCAR (which is similar to that under MiFID II) and that of a "client" under art. 4(1) IFR (which applies to MiFID II proprietary traders), "clients" within the meaning of MiCAR do not include "counterparties".

III under the first proposal text of MiCAR of the Commission, art. 77(1) MiCAR (then art. 69(1) MiCAR) included the term "crypto-asset provider" instead of "crypto-asset *service* provider", perhaps indicating the lack of a service element and therefore leaning towards a CASP *activity*. However, the other paragraphs of the article did use the full term CASPs, wherefore we consider that to have been a textual error without deeper meaning.

IV in the European Commission's original proposal, art. 3(1)(12) and (13) MiCAR, comprising the definition of the service in question, the service was defined as "concluding purchase or sale contracts concerning crypto-assets with **third parties** [...]". Based on this change it seems that traditional proprietary trading was meant to be excluded from the scope of MiCAR by the EU legislature, seeing as the change from *third-parties* to *clients* could be seen as a policy shift.

Similar to the guidance of the European Commission in respect of MiFID II, we would believe that an indication of whether a proprietary trader has to identify a counterparty as a client would be *inter alia* the extent to which such party is known to the proprietary trader and whether the proprietary trader voluntarily decides on executing a transaction. Admittedly, this indicator would be skewed towards on-exchange trading, where no discretionary rules on order execution may exist. However, we do not directly see how a proprietary trader that on an OTC-basis enters into specific (contractual) transactions with counterparties is not providing the regulated service of exchanging crypto-assets for funds or other crypto-assets.

For example, we consider it foreseeable that crypto-asset dealings of systematic internalisers[32] would fall under this service. The more the proprietary trader presents itself to the outside world as willing to deal against own account outside a trading venue, the more likely it will be that the proprietary trader would be in scope of the CASP authorisation requirement.

However, determining whether a counterparty of a proprietary trader would qualify as a "client" on the basis of whether the counterparty legitimately relies on the CASP to protect its interests (e.g., on the basis of the European Commission's guidance in respect of MiFID II) seems problematic as a positive answer to that question would correspondingly mean that the service likely also involves MiCAR Order Execution. In this context, we note that Recital 87 of MiCAR recognises that when a CASP executing orders for crypto-assets on behalf of clients is the client's counterparty, there might be similarities with the services of exchanging crypto-assets for funds or other crypto-assets. However, MiCAR stipulates that in exchanging crypto-assets for funds or other crypto-assets, the price for such exchanges is freely determined by the CASP as a currency exchange. Yet in the execution of orders for crypto-assets on behalf of clients, the CASP should always ensure that it obtains the best possible result for its client, including when it acts as the client's counterparty, in line with its best execution policy. Perhaps even more impactful for proprietary traders would be the potential loss of flexibility in their remuneration policy, as awarded to them under the (Dutch implementation of the) MiFID II regime.[33]

Interestingly, the rationale behind regulating exchanging crypto-assets for funds or other crypto-assets seems to (partly) stem from a need for consumer protection. For example, MiCAR requires CASPs that exchange crypto-assets for funds or other crypto-assets by using their own capital to draw up a non-discriminatory commercial policy to ensure consumer protection. Traditional proprietary traders (e.g., market makers or participants in or members of regulated markets or MTFs) however interact exclusively with non-consumers. Despite this reference to consumer protection in the recitals, MiCAR makes, contrary to MiFID II, no distinction between eligible counterparties, professional clients or retail clients, and the relevant MiCAR requirements (e.g., best execution requirements) apply to all clients regardless of their capital or level of experience.

[32] Art. 4(1)(20) MiFID II.

[33] Specifically art. 1:121(7)(c) FSA.

All in all, if proprietary traders that hold an investment firm licence are understood to conduct the "exchange of crypto-assets for funds or other crypto-assets" if they conduct their activities in respect of crypto-assets, they must go through the notification procedure and are subject to certain MiCAR requirements. In view of the upcoming deadline and limited transitional period under the grandfathering regime, we deem it of the utmost importance for proprietary traders that the precise demarcation of this crypto-asset service *vis-à-vis* MiFID II proprietary trading is clarified by means of supervisory guidance.

3.3.2.2 Payment services

Depending on how a payment process between a CASP and credit institutions is structured, the business operations of a CASP may also involve the provision of a payment service within the meaning of the Payment Services Directive 2 ("**PSD2**")[34] when offering one or more crypto-asset services (e.g., the provision of transfer services for crypto-assets on behalf of clients). MiCAR does however not clarify when CASPs engage in the provision of regulated payment services when offering crypto-asset services.

In this context, it is relevant to note that Recital (82) of MiCAR stipulates that CASPs should be authorised to make payment transactions in connection with the crypto-asset services they offer '*only where they are authorised as payment institutions in accordance with PSD2.*' Similarly, art. 70(4) MiCAR stipulates that CASPs may themselves, or through a third party, provide payment services related to the crypto-asset service they offer, provided that the CASP itself, or the third party, is authorised to provide those services under PSD2. Where they provide such payment services, CASPs must inform their clients of: (a) the nature and terms and conditions of those services, including references to the applicable national law and to the rights of clients; and (b) whether those services are provided by them directly or by a third party.

Although the official Dutch translation of MiCAR seems to suggest that CASPs may only provide payment services: (i) if they themselves hold; or (ii) through a third party that holds, a licence as a payment institution under PSD2 (i.e., suggesting they may not use banks or electronic money institutions as such third parties), we consider it to be the better view that the relevant article also intends to cover those parties that are otherwise authorized to provide payment services (i.e., banks or electronic money institutions).

[34] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.

That being said, the reference to "authorised to provide those services under PSD2" in our view suggests that a third party that provides payment services under an exemption (e.g., the exemptions under art. 3 PSD2) falls outside the scope of art. 70(4) MiCAR, meaning that a CASP cannot rely on such party if it wishes to use that party to provide payment services related to its crypto-asset services.

3.3.3 Timing

The regulated financial undertakings that wish to provide crypto-asset services by using the notification regime, must notify the AFM of certain information (as further set out in Section 9) at least 40 working days before providing its services. The AFM must, within 20 working days of receipt of such notification, assess whether all required information has been provided.

3.4 Passporting procedure

In order to start providing crypto-asset services on a cross-border basis in other EU Member States under the passporting regime, a CASP must submit the following information to its home Member State supervisor:[35]

I a list of the Member States in which the CASP intends to provide crypto asset services;

II the crypto-asset services that the CASP intends to provide on a cross-border basis;

III the starting date of the intended provision of the crypto asset services; and

IV a list of all other activities provided by the CASP not covered by MiCAR.

The home Member State supervisor must, within 10 working days of receipt of said information communicate that information to the single point of contact of the host Member State, to ESMA and to the European Banking Authority ("**EBA**"). The supervisor of the Member State that granted authorisation must inform the CASP of this communication without delay. The CASP may then begin to provide its services in the host Member State from the date of receipt of said communication or at the latest from the 15th calendar day after having submitted the information.

[35] Art. 65 MiCAR.

It must be noted that CASPs providing services under the grandfathering regime (see Section 3.2.1) will not be able to use the passporting regime, which is solely available to CASPs authorised under MiCAR, except where host Member States indicated that they accept such cross-border service provision for the duration of their grandfathering regime.[36] Once authorised, CASPs providing services on a cross-border basis within the EU will not be required to have a physical presence in the host Member States where they provide their services.[37]

3.5 Reverse solicitation

Under MiCAR, it is possible for CASPs located in third-countries to provide crypto-asset services to EU customer, provided that the EU customer initiates the provision of the service or activity at its own exclusive initiative (i.e., reverse solicitation).[38] The rationale behind this is that where a third-country firm provides crypto-asset services on the own initiative of a customer established in the EU, the crypto-asset services should not be deemed to be provided in the EU and thus not be in scope of MiCAR. However, ESMA has already indicated with considerable force that it, and its member national competent authorities (e.g., the AFM), plan to take a very strict interpretation of this provision, which interpretation will be disclosed in the third RTS package due in Q1 2024. How this will exactly play out in the highly decentralised ecosystem of crypto-asset services remains to be seen.[39] However, if the Binance case[40] is anything to go by, we deem it extremely difficult for unauthorised entities to provide their services in the EU without being authorised to do so under MiCAR.

We also note that the Dutch supervisors are usually disinclined to assume that regulated services are provided at the sole initiative of the client. Generally, the reverse solicitation exemption is more likely to be successfully relied upon if: (i) a third-country institution has no more than a few Dutch clients; (ii) the exemption is only used in individual cases; and (iii) the institution has no presence in the Netherlands at all. Hence, we generally advise against relying on reverse solicitation as a business model to provide services to Dutch clients.

[36] ESMA Q&A 2086.

[37] Art. 59(7) MiCAR.

[38] Art. 61 MiCAR and Recital (75); ESMA will provide specific guidance on the reverse solicitation test in to be drafted Guidelines, of which the first draft version is anticipated in Q1 2024.

[39] Reference is made to the ESMA Consultation Paper on the draft guidelines on reverse solicitation under the Markets in Crypto Assets Regulation (MiCA), (2024).

[40] DNB, Besluit tot het opleggen van een bestuurlijke boete aan Binance, (2022).

3.6 Other exemptions

MiCAR also provides for other exemptions to the CASP authorisation regime (e.g., an intra-group exemption).[41] However, these exemptions are outside the scope of this White Paper given that this White Paper primarily seeks to address the provision of crypto-asset services that are in-scope of MiCAR and which are, thus, subject to an authorisation requirement. We furthermore believe it to be the better view that, if a party seriously wishes to provide crypto-asset services to EU customers, the authorisation or notification procedure will almost undoubtably be the only viable business strategy from a regulatory perspective.

[41] Art. 2(2)(a) MiCAR.

4. GOVERNANCE REQUIREMENTS

4. GOVERNANCE REQUIREMENTS

4.1 Introduction

CASPs are subject to a broad range of governance requirements, which are generally similar to those applicable to investment firms. In the Netherlands, governance requirements applicable to regulated entities (e.g., investment firms) have mainly been implemented in Dutch law by means of principle-based provisions[42], requiring regulated entities to have a controlled and sound business organisation. As MiCAR is a directly applicable Regulation, these national provisions are not directly applicable to CASPs.[43] This leads to interesting discrepancies. For example, MiCAR does not require the creation of risk or compliance functions nor the instatement of an internal audit function. However, in view of the rules applicable to other regulated entities it could be considered best practice for CASPs to apply a similar internal governance structure as other regulated entities (i.e., a form of three-lines of defence model). Due to the frequent mentioning of sufficient resources that must be allocated to a certain policy or area of governance in MiCAR, it seems furthermore practical for CASPs to create a 'compliance' function observing all these requirements.

The various governance requirements applicable to the authorisation regime have been set out in more detail below.

4.2 Fit and proper requirements

The fit and proper requirements for the management (and supervisory) body of the CASP stipulate that the members thereof must have sufficient time, be of sufficiently good repute and possess the appropriate knowledge, skills and experience, both individually and collectively, to perform their duties. In particular, members of the management body of CASPs may not have been convicted for any offences relating to money laundering and terrorism financing ("**ML/TF**") or for any other offences that would affect their good repute.[44]

[42] For example, art. 3:17 and 4:14 FSA.

[43] This is particularly interesting where regulated entities are providing crypto-asset services as they are not exempted from the governance requirements ex art. 68 MiCAR. This would mean that in essence a firm might be subjected to two parallel governance regimes, which shall be equivalent to a large extent, although never fully aligning.

[44] Art. 68(1) MiCAR.

The strong focus of MiCAR on the fit and proper assessment seems to be a reflection on the questionable staffing of certain crypto-asset players, particularly those involved in the recent malversations in the crypto-sector. A CASP must therefore provide proof that members of its management body are of sufficiently good repute and possess the appropriate knowledge, skills and experience and sufficient time to manage its business.

The AFM identifies that in course of a CASP authorisation, the following fit and proper documentation must be provided:[45]

Table 3

#	Document	#	Document
1	Prospective appointment notification form (always applicable, even when already appointed) *NB. After authorisation, as part of ongoing supervision, board members first need to be tested before they can be appointed*	6	Suitability matrix for supervisory board members (if applicable)
2	Integrity screening form (only if not previously screened by the AFM or DNB or in case of new relevant facts after previous screening)	7	Standardized curriculum vitae
3	Statement no new relevant integrity related facts (only if previously screened by the AFM or DNB)	8	Copy ID
4	Suitability matrix for policy makers *Including questions on knowledge of relevant regulations, so we expect substantiation on adequate knowledge on MiCAR, AML/TFR, DORA, etc.*	9	Considerations regarding appointments
5	Job profile		

Whilst for certain documents the final version is yet to be made available, the AFM indicated it will include certain MiCAR specific questions, for instance with regards to Digital Operational Resilience Act ("**DORA**")[46] and ML/TF topics. The question is to what extent these are truly MiCAR specific questions, and whether the implementation of these requirements in a crypto-asset environment require certain peculiarities, different from those of *regular* financial services.

[45] Art. 62(3) and 68(1) MiCAR.

[46] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

Insofar regulated entities were not already subject to such requirement, art. 69 MiCAR ensures that if any change in the management body of a crypto-asset service providing entity occurs, must notify its competent authority forthwith, prior to the exercise of activities by any new members. Seemingly, this could mean that in *ex post* jurisdictions where the fit and proper assessment takes place after the appointment of the board member, such as in Germany, a prior approval regime will apply based on the MiCAR, being a directly applicable EU Regulation, at least precluding the new board member from performing any activities before the notification has occurred. We however read this provision in such a manner that: (i) the notification of the change itself; and (ii) the provision of the necessary information to assess compliance with art. 68 MiCAR is sufficient to meet the notification requirement, i.e., rather than that the full fit and proper assessment procedure must be completed at the time of the notification.

Persons (or board members of legal entities) having a qualifying holding in a CASP (reference is made to Section 6) are equally subject to the propriety assessment, whereby these persons may be subject to potential limitations on the exercise of their voting rights or penalties if they are deemed to be prejudicial to the sound and prudent management of the CASP.[47] Additionally, CASPs are required to employ personnel with adequate knowledge, skills and expertise to discharge their responsibilities. Whereas investment firms can rely on respected certification schemes or educations in the fulfilment of similar requirements under MiFID II, CASPs have to carefully consider what they consider to be qualified personnel and whether their competent authority would share such views.[48] We therefore consider it to be the better view that the CASP must draft a policy on the suitability of its employees, including at least a requirement for some form of annual training or certification.

4.3 Corporate information

As with any application for a licence or authorisation, it must be clear to the supervisor who the applicant is and thus the supervisee. To that end, applicants have to submit: (i) their name, including the legal name and any other commercial name used; (ii) the legal entity identifier of the applicant CASP; (iii) the website operated by that provider and contact information; (iv) the legal form of the applicant CASP; and (v) the articles of association (where applicable).

[47] Art. 68(2) and (3) MiCAR.

[48] Art. 68(5) MiCAR.

Whilst this requirement will be relatively straightforward for most applicants, interesting issues could arise when trying to meet this requirement for DeFi applications. Theoretically, MiCAR steers clear of DeFi, with a review of its implications by ESMA being due on 30 December 2024.[49] However, perhaps paradoxically, MiCAR draws certain decentralised applications within its scope by means of its recitals, stating that: *'This Regulation should apply to natural and legal persons and certain other undertakings, [...] including when part of such activities or services is performed in a decentralised manner.'* What exactly is to be understood as *certain other undertakings* and services performed in a *partly decentralised manner* is not entirely clear and it is yet to be seen whether there will be cases qualifying under this *nomer* any time soon. In any event, undertakings that are not legal persons are only permitted to provide crypto-asset services if their legal form ensures a level of protection for third parties' interests equivalent to that afforded by legal persons and if they are subject to equivalent prudential supervision appropriate to their legal form.[50]

Practically, no (partly) DeFi application will likely proactively seek authorisation as a CASP, seeing as the very concept is meant to avoid the risk of a licensed intermediary materialising. Rather, we expect this category to predominantly be a tool for the supervisor to enforce MiCAR in respect of (third-country) parties that seek to circumvent the rules.[51]

CASPs should have their registered office in the EU, or operate from the EU if they are not legal persons.[52] At least part of the CASP's crypto-asset services need to be provided from the EU.[53] Furthermore, at least one (1) of the directors of the CASP should be resident in the EU and the effective management, i.e., the daily policy making, needs to take place in the EU.

[49] Art. 142(2)(a) MiCAR.

[50] Art. 59(3) MiCAR.

[51] An interesting example is given by ESMA itself in respect of decentralized exchanges ("**DEXs**") and pre-trade transparency: 'Finally, regarding DEXs, ESMA acknowledges Recital 22 of MiCAR that "(...) Where crypto-asset services are provided in a fully decentralised manner without any intermediary" should fall outside the scope of MiCAR but also notes that the exact scope of this exemption remains uncertain. ESMA considers that an assessment of each system should be made on a case-by-case basis considering the features of the system.'

[52] Recital (74) MiCAR.

[53] Art. 59(2) MiCAR.

4.4 Programme of operations

The programme of operations is a document wherein the applicant describes the crypto-asset services it wishes to provide with a sufficient level of granularity. The programme of operations should (at least) cover the first three (3) years upon authorisation, allowing the supervisor to make a forward-looking assessment.[54] ESMA expects the programme of operations to cover a wide range of topics such as: (i) the services to be provided; (ii) marketing plan; and (iii) the CASP's group structure, affiliated entities, outsourcing arrangements and intra-group financial links.[55] This expansion must be seen as an effort to bring more clarity and control over groups active in the crypto-markets. To that end, ESMA requires the programme to comprise information on the activities and services of CASP group entities, which – insofar relevant – are to be represented in the accompanying outsourcing policy. This feels like a consolidated application of MiCAR, whereas MiCAR itself does not foresee in a prudential consolidation regime.

All in all, the programme of operations as it stands will be a large document that describes a plethora of (un)regulated activities of the CASP and its group entities. It requires careful drafting and should in our view be seen as the central piece of documentation in the authorisation application procedure. Although the draft ITS may still be subject to change, it seems that this particular provision requires CASPs to have a clear and convincing projection of their operations and a solid reasoning as to why such operations ought to be authorised. To what extent a CASP is bound to its initial programme of operations when it decides to deploy activities outside of the scope described therein, is not foreseeable. Technically, however, such plan is never binding and merely serves as an indication of the services offered. In principle, once a CASP is authorised for a certain crypto-asset service, it may offer it in any variety it deems fit for as long as it continues to comply with the regulatory requirements.

[54] Art. 62(2)(d) MiCAR and art. 2 Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included in a notification by certain financial undertakings of their intention to provide crypto-asset services.

[55] ESMA, 2023a, paragraph 31.

4.5 Internal governance policy

CASPs have to draft internal governance policies and procedures that implement a system of control, which is broadly equivalent to the *three lines of defence model* applied by most other financial undertakings. During the *crypto winter* several significant governance failures were identified, prompting ESMA to emphasise the relevance of proper internal safeguards. Thus, a CASP must clearly and in a detailed manner describe its governance division, setting out which business functions are responsible for which controls, the reporting lines and certain professional information on responsible staff (e.g., CV, and a description of their skills and knowledge). Moreover, the manner in which the independence of the control functions is guaranteed must be described so as to ensure that these functions can discharge their controlling functions in an adequate manner. It must be noted however, that MiCAR does not require the creation of separate risk and compliance functions, instead permitting the creation of a single *control* function.

We consider it to be the better view that for the internal governance, MiFID II/ Investment Firm Directive ("**IFD**")[56] or Capital Requirements Directive ("**CRD IV**")[57] compliant arrangements would generally be MiCAR compliant arrangements and that there should not be a major additional burden for regulated entities in this respect. In that light, it should be taken into account that MiCAR generally has a less intensive scope than other regulatory instruments. It is a complicating factor that the MiCAR governance rules are based on a directly applicable Regulation, whereas under most other regulatory instruments the governance provisions stem from Directives that have been transposed into national law.

4.6 AML/CTF policies and procedures

The requirement for CASPs to have adequate anti-money laundering and counter terrorist financing ("**AML/CTF**") policies and procedures is not new. Currently, under the AMLD5 framework, CASPs are already required to have a policy in place that supports the detection and prevention of ML/TF.

[56] Directive (EU) 2019/2034 of the European Parliament and of the Council of 27 November 2019 on the prudential supervision of investment firms.

[57] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions.

Under MiCAR, the requirements are further expanded commensurate to the more intensive nature of the applicable supervision.[58] It must be noted that CASPs are also subject to the relatively far-reaching consequences of the new Transfer of Funds Regulation ("**TFR**")[59], requiring CASPs to attach certain information to transfers of funds and crypto-assets, even if such transfers solely occur in a domestic setting. It may be required for CASPs to have advanced detection methods to track the parties involved in a crypto-asset transaction for it to be able to offer services in respect of certain (anonymous) crypto-assets.

4.7 Business continuity policy and plan

In order to ensure the continued robustness of the CASP's business, sufficient detail on the business continuity arrangements, plans and measures must be provided in the form of a business continuity policy.[60] This description must include, among others, a periodic testing of the adequacy of the plan including an assessment of the criticality or importance of functions supported by third-party providers.[61] ESMA recognises that the best practices for business continuity arrangements with respect to crypto-asset services have yet to crystallise, however, it identifies points such as *lock-in* risk and unpredictable DLT governance decisions as possible disruptive events.[62]

A business continuity policy must include all of the following elements[63]:

I a definition of the scope, including limitations and exclusions, to be covered by the business continuity plans, procedures and measures;

II a description of the criteria to activate the business continuity plans;

III provisions on the governance and organisation including roles, responsibilities and escalation procedures to implement the business continuity policy and to ensure that sufficient resources are available;

[58] Art. 68(8) MiCAR.

[59] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets.

[60] Art. 68(7) MiCAR.

[61] Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) No 2023/1114 of the European Parliament and of the Council on markets in crypto-assets with regard to regulatory technical standards on continuity and regularity in the performance of crypto-asset services.

[62] ESMA, 2023b.

[63] Art. 3 of Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) No 2023/1114 of the European Parliament and of the Council on markets in crypto-assets with regard to regulatory technical standards on continuity and regularity in the performance of crypto-asset services.

IV provisions on the alignment between the general business continuity plans and the ICT-specific business continuity plans, and ICT response and recovery plans;

V provisions on the review of the effectiveness of the implemented business continuity plans.

The business continuity plans included in the policy must also account for the possible event that the quality of the provision of such functions deteriorates to an unacceptable level or fails. The business continuity plans must provide for the following minimum content:[64]

I a range of possible adverse scenarios relating to the operation of critical or important functions, including the unavailability of business functions, staff, workspace, external suppliers or data centres or loss or alteration of critical data and documents;

II the procedures and policies to be followed in case of a disruptive event, including necessary measures to recover critical or important functions consistent with recovery time objectives and recovery point objectives and the maximum time to resume services;

III procedures and policies for relocating the business functions used to provide crypto-asset services to a back-up site;

IV back-up of critical business data including up-to-date information of the necessary contacts to ensure communication within the CASP, between the CASP and its clients and between the CASP and the infrastructures on which its services rely;

V procedures for timely external communications with clients in the event of a disruption involving a permissionless distributed ledger used by the CASP in the provision of its services. The CASP shall ensure that the communication to clients includes information on when the services are expected to be resumed, on the reasons and the impact of the incident, and on risks concerning clients' funds and crypto-assets held on their behalf;

VI the business continuity plans must set out procedures to address any disruptions of outsourced critical or important functions, including where those critical or important functions become unavailable.

[64] Art. 4 of Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) No 2023/1114 of the European Parliament and of the Council on markets in crypto-assets with regard to regulatory technical standards on continuity and regularity in the performance of crypto-asset services.

CASPs must periodically, but at least once a year, assess whether the business continuity plans are still adequate and up-to-date, potentially by means of a third-party audit.[65] Moreover, CASPs have to design their business continuity policy and plans in a manner that is proportional to their complexity and risks, which they shall verify annually by means of a self-assessment.[66]

4.8 ICT risk and operational resilience policy

In light of the requirement of art. 62(2)(j) MiCAR, MiCAR explicitly refers to the requirements of DORA to ensure the continuity and regularity of the performance of the (essential)[67] crypto-asset services.[68] Comprising the obligation to draft an ICT business continuity plan (separate from the one above), an ICT response and recovery plan and a ICT risk management policy, safeguarding the preservation of essential data and functions and the maintenance of crypto-asset services or, if need be, the timely recovery of such data and functions and the timely resumption of crypto-asset services.[69]

4.9 Data retention policy

A data retention policy providing insights into all crypto-asset services, activities, orders, and transactions undertaken by the CASP. Such data must be retained for five (5) years or for seven (7) years if requested to do so by the relevant supervisor.[70]

[65] Art. 5 of Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) No 2023/1114 of the European Parliament and of the Council on markets in crypto-assets with regard to regulatory technical standards on continuity and regularity in the performance of crypto-asset services.

[66] Art. 6 of Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) No 2023/1114 of the European Parliament and of the Council on markets in crypto-assets with regard to regulatory technical standards on continuity and regularity in the performance of crypto-asset services.

[67] What is to be understood as essential crypto-asset service becomes highly interesting as the definition of critical or important function of DORA does not seem to perfectly align with the paradigm that crypto-asset services are (currently) not systemically important.

[68] Art. 68(7) MiCAR.

[69] Ibid.

[70] Art. 68(9) MiCAR.

4.10 Complaints-handling procedures

Akin to the obligation for investment firms under MiFID II, CASPs have to establish and maintain effective and transparent complaints handling procedures that safeguard the prompt, fair and consistent handling of complaints received from clients.[71] This enables clients to submit complaints for free, based on a template offered by the CASP, upon which the CASP must respond in a fair, understandable and timely manner. Due to the novel nature of the services offered, and the relatively large (proven) potential for loss of investments, clients are expected to submit a substantial amount of complaints to CASPs. Therefore, ESMA has seen fit to take a detailed approach in its draft RTS on the requirements surrounding complaints handling, including a standardised complaints report template.[72]

In any case, the complaints handling policy must ensure that: (i) sufficient human and technical resources are being dedicated to the handling of complaints; (ii) the persons in charge of the procedure have sufficient knowledge and skills; and (iii) clients are sufficiently informed and enabled to file a complaint free of charge.

4.11 Conflicts of interest policy

The ongoing litigation surrounding the failure of FTX made clear that conflicts of interest are not only severe in the crypto-asset ecosystem, they are also plentiful. Therefore, MiCAR requires CASPs to implement and maintain effective conflict of interest policies and procedures, taking into account the scale, the nature and range of the services provided.[73] The conflicts policy should be clearly and adequately disclosed on the CASP's website and should address conflicts between:[74]

[71] Art. 71 MiCAR. Not unsimilar to the requirements under art. 16(2) MiFID II and art. 26 DR MiFID II.

[72] Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards on the requirements, templates and procedures for handling complaints by CASPs.

[73] With art. 79(2) MiCAR providing for more conflict of interest requirements for CASPs placing crypto-assets. Whatever the proportionality included in this article may mean, it shall never be able to be constructed that smaller CASPs shall be allowed to operate without mitigating conflicts. See also recital (79) MiCAR.

[74] Art. 72(1), (2) and (3) MiCAR.

I CASPs and: (a) their shareholders or members; (b) any person directly or indirectly linked to the CASP or their shareholders or members by control; (c) members of their management body; (d) their employees; or (e) their clients; or

II two (2) or more clients whose mutual interests conflict.

Conflicts of interest can be roughly delineated into three groups, being: (i) conflicts of interest between the CASP and its clients; (ii) the conflicts of interest between individual clients or groups of clients of the CASP; and (iii) conflicts of interests that may prevent persons or entities linked to the CASP, i.e., internal conflicts of interests. Conflicts of interest, including those arising from personal transactions, should be prevented and/or be managed insofar they arise in accordance with the conflicts policy, where disclosure alone does not suffice as a mitigant. ESMA has, based on the mandate given to it, drafted RTS that specifically target conflicts of interest, containing a large amount of detail.[75] Interestingly, ESMA mentions that remuneration policies may be specific points of attention for the mitigation of conflicts, whilst MiCAR otherwise remains silent on remuneration policies. The draft RTS contain specific provisions on the remuneration policy, however, to what extent ESMA is overstepping its mandate remains to be seen and we consider it not fully unlikely that these rules may be adapted.[76] In any case, the management board remains responsible and sufficient resources have to be allocated.

4.12 Outsourcing policy

In line with the general trend of more attention for outsourcing, MiCAR contains a specific provision for the subject, in addition to the provisions of DORA to which CASPs are subjected.[77] CASPs that outsource services or activities to third parties for the performance of operational functions must take all reasonable steps to avoid additional operational risk, including stipulating the requisite contractual safeguards in outsourcing agreements.[78]

[75] Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards on the requirements for the policies and procedures of CASPs to identify, prevent, manage and disclose conflicts of interest as well as on the details and methodology for the content of disclosures of conflicts of interest.

[76] Art. 5 Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included in a notification by certain financial undertakings of their intention to provide crypto-asset services.

[77] Art. 73 MiCAR and art. 2(1)(f) DORA.

[78] Art. 73(3) MiCAR.

The outsourcing policy must, on a proportional basis, at least ensure that:

I outsourcing does not result in the delegation of responsibilities of the CASP;

II outsourcing does not alter the relationship between the CASP and its clients, nor the obligations of the CASP towards their clients;

III outsourcing does not alter the conditions for the authorisation of the CASP;

IV third parties involved in the outsourcing cooperate with the competent authority of the CASP and the outsourcing does not prevent the exercise of the supervisory functions of competent authorities, including on-site access to acquire any relevant information needed to fulfil those functions;

V the CASP retains the expertise and resources necessary for evaluating the quality of the services provided, for supervising the outsourced services effectively and for managing the risks associated with the outsourcing on an ongoing basis;

VI the CASP has direct access to the relevant information of the outsourced services;

VII the CASP ensures that third parties involved in the outsourcing meet the data protection standards of the EU, such as the GDPR.[79]

4.13 Wind-down plan

CASPs are obliged to draft orderly wind-down plans, wherein they set out and demonstrate their ability to orderly wind down their services and activities without causing undue harm to their clients, whereby they ensure that any critical activities or services provided by the CASP are continued.[80] In practice, such a wind-down plan requires considerable drafting and a certain capital buffer to cover the costs of the process. Whilst these may well be covered by the prudential requirements, an internal buffer may have to be maintained by the CASP to satisfy the supervisor.

[79] Art. 73(1) MiCAR.

[80] Art. 74 MiCAR.

4.14 Other general policies

As a general rule, CASPs have to draft policies that ensure their continued effective compliance with MiCAR in the broad sense.[81] Such documentation includes the accounting policy, compliance charter, whistleblowing policy, audit charter (if applicable) and other miscellaneous documentation. These policies must to a large part be based on existing IFD/MiFID II policies or similar documents.

4.15 Selected service specific policies

Below, the requirements for the provision of selected specific crypto-asset services are briefly described, with the exception of the safeguarding and administration service, which is dealt with in Section 7.

4.15.1 Operation of a crypto-asset trading platform

CASPs seeking authorisation for the operation of a crypto-asset trading platform must provide, on top of all other required information described above, submit a description of the operating rules of the trading platform and of the procedure and system to detect market abuse.[82] This required information corresponds to that generally included in market rulebook for MTF and OTF operators under MiFID II. The minimum content of the rulebook must be:

I the admission to trading of crypto-assets (including information on exclusion, fees, due diligence requirements, non-discriminatory rules for the access to trading);

II the trading of those crypto-assets (including liquidity thresholds, periodic disclosure requirements, suspension grounds etc. and the rules governing the execution, cancellation and routing of orders);

III the settlement of those crypto-assets (including details on when a trade settlement is considered to be final, all verifications required to ensure the settlement of the trades occur and measures with regards to settlement fails).

[81] Art. 68(4) and (6) MiCAR.

[82] Art. 62(2)(n) MiCAR; see also ESMA, 2023b, paragraphs 129-133.

CASPs operating a trading platform are also charged with assessing the suitability of any issuer seeking admission to trading of their crypto-assets on the trading platform.[83] This assessment comprises an evaluation of the reliability of the technical solutions used and the potential association to illicit or fraudulent activities, taking into account the experience, track record and reputation of the issuer of those crypto-assets and its development team. This puts the CASP in the role of the supervisory authority in financial markets, who are charged with authorising the prospectus of an issue, raising questions as to the potential liability of the trading platform.

Special attention should be paid to the fact that CASPs operating a trading platform shall have to develop procedures to detect and prevent market abuse, pursuant to the *sui generis* market abuse rules of Title VI MiCAR.[84] These rules are largely based on the MAR[85] and MAD[86] and cover topics such as insider dealing and market manipulation, who have been primarily lifted from these regulations and adjusted somewhat to be directly fitted within the MiCAR. Thus, existing knowledge of the MAR is highly relevant, yet should not be mechanically relied upon when drafting MiCAR market abuse documentation. The MiCAR market abuse Title does differ, however, from the MAR in the sense that it must be seen as a light-version of the highly detailed regime applicable to financial instruments.

4.15.2 The exchange of crypto-assets for funds or other crypto-assets

This service, equated with the MiFID II service of dealing on own account, requires CASPs to provide information on their non-discriminatory commercial policies setting out their trading practices.[87] This comprises elements such as the types of clients with whom and under what circumstances the CASP is willing to deal, the pricing and the manner in which the CASP quotes those prices for trading and the moment in which trades will be executed. Moreover, CASPs will be subject to trade transparency requirements dictating the publication of information such as volume and prices of an executed trade (see Section 8).[88]

[83] Art. 76(2) MiCAR.

[84] Art. 92 MiCAR.

[85] Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse.

[86] Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse.

[87] Art. 77(1) MiCAR. A distinction should be made to situations where the CASP is dealing on behalf of a client and is itself a counterparty to that client, which shall be governed by the best-execution policy and situations where a CASP converts crypto-assets for funds, which shall be done at a rate freely determined by the CASP, see Recital (87).

[88] Art. 77(4) MiCAR.

4.15.3 Execution of orders on behalf of third-parties

This service is subject to similar rules as those surrounding the concept of *best execution* in the MiFID II.[89] CASPs have to take all necessary steps to obtain, while executing orders, the best possible result for their clients taking into account factors of price, costs, speed, likelihood of execution and settlement, size, nature, conditions of custody of the crypto-assets or any other consideration relevant to the execution of the order.[90] The manner in which the CASP seeks to fulfil this best execution requirement must be laid down in a execution policy, setting out details such as a list of trading platforms used specified per category of crypto-asset, the consideration of factors such as speed, costs, likelihood of settlement, size, nature and the conditions of custody of the crypto-assets in addition to any other relevant factors.

The execution policy must be disclosed, or information on the execution policy must be disclosed to, the client in a clear and understandable manner. Once shared with the client, a CASP will have to obtain *consent* from each and every client on the execution policy, before executing any trades on behalf of that client.[91] A CASP must also on an ongoing basis: (i) verify to what extent its execution policy is effective in getting the best possible transactions for its clients; and (ii) inform the client if a material change occurs in light of an adjustment to the execution policy.

4.15.4 Providing advice on crypto-assets

Briefly put, CASPs offering advisory services to their clients have to draft a suitability policy[92] and a knowledge training policy, respectively: (i) detailing the manner in which information is gathered and assessed to ascertain the suitability of the crypto-asset for the client; and (ii) the manner in which the sufficient knowledge of the advisors is safeguarded and the resources made available by the CASP for the training of its staff.

[89] Art. 27 MiFID II and 64 et seq. Commission Delegated Regulation (EU) 2017/565 of 25 April 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council as regards organizational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive.

[90] Art. 78(1) MiCAR.

[91] Art. 78(3) MiCAR.

[92] Art. 81(10) MiCAR.

4.15.5 Transfer services for crypto-assets

In addition to the transfer service agreement, setting out the details and modalities of the service to be provided, that must be concluded by the CASP with the client, the CASP providing this service must draft a policy setting out: (i) the types of crypto-assets for which the applicant intends to provide transfer services; (ii) the arrangements and resources to address risks quickly, efficiently and thoroughly during the whole process of providing transfer services, including operational failures and cybersecurity risks; (iii) insofar applicable a description of the CASP's insurance policy; and (iv) information supply to its clients on the transfer service policy.

5. PRUDENTIAL REQUIREMENTS

5. PRUDENTIAL REQUIREMENTS

CASPs are subject to certain prudential requirements with the ultimate goal of consumer protection, not necessarily as a safeguard to financial stability.[93] This narrow regulatory goal is reflected in the prudential requirements of MiCAR. These are a slimmed-down version of those applicable to investment firms under the Investment Firm Regulation ("**IFR**"),[94] where the European legislature has chosen to forego the complicated regime of the K-factor requirements, and which seek to cover the risk profile of the investment firm itself. Instead, the capital requirement for a CASP is the higher of:[95]

a the amount of permanent minimum capital requirements indicated in Annex IV to MiCAR, depending on the type of the crypto-asset services provided; or

b one quarter of the fixed overheads of the preceding year, reviewed annually. With the fixed overheads being the total costs over the previous year minus certain deduction posts.[96]

The capital requirement must be met by means of holding Common Equity Tier 1 ("**CET1**")[97] capital or taking out an insurance policy (or equivalent guarantee).[98] It is important to note that all of the deductions from CET1 items of art. 36 of the Capital Requirements Regulation ("**CRR**")[99] apply, with the exception of the threshold exemptions of art. 46 and 48 CRR. This means that different deductions apply to investment firms than to CASPs, where investment firms have to apply less

[93] Recital (80) MiCAR.

[94] Regulation (EU) 2019/2033 of the European Parliament and of the Council of 27 November 2019 on the prudential requirements of investment firms.

[95] Art. 67(1) MiCAR.

[96] The methodology of calculating the fixed overheads requirement principally follows the subtractive methodology of art. 13 IFR, however, it contains a significantly restricted set of deduction posts that need to be deducted from the total costs in art. 67(3) MiCAR, where there also have not been drafted any RTS further specifying these deductions, as is done for investment firms by means of Delegated Regulation (EU) 2022/1455. Art. 67 MiCAR does not contain a delegation power for the Commission to do so either, which raises the question why the legislature chose to be so strict on this deductions regime, which contrary to the IFR's regime does not seem to drafted as an open-ended list but rather a limitative set of deductions.

[97] Defined in accordance with art. 26 to 30 of the Capital Requirements Regulation (EU) 575/2013 pursuant to art. 67(4) (a) MiCAR and thus requiring a careful drafting in order to be eligible as CET1.

[98] Which, pursuant to art. 67(5) MiCAR, shall at least: (i) have an initial term of not less than one year; (ii) a notice period of at least 90 days; (iii) be taken out from a (Solvency II) insurer; and (iv) provided by a third-party entity. The insurance provides cover against: (a) loss of documents; (b) misrepresentations or misleading statements made; (c) acts, errors or omissions resulting in a breach of: (i) legal and regulatory obligations; (ii) the obligation to act honestly, fairly and professionally towards clients; (iii) obligations of confidentiality; (d) failure to establish, implement and maintain appropriate procedures to prevent conflicts of interest; (e) losses arising from business disruption or system failures; (f) where applicable to the business model, gross negligence in the safeguarding of clients' crypto-assets and funds; (g) liability of the CASPs towards clients pursuant to art. 75(8) MiCAR.

[99] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions.

deductions, although arguably, the deductions are to a lesser extent relevant to the business model of CASPs. For instance, they will not be expected to regularly come into possession of other regulatory own funds instruments.[100] In the draft RTS, ESMA specifies that the CASPs will need to provide forecasted own funds calculations in accordance with art. 67 MiCAR for the coming three (3) years when applying for an authorisation.[101]

In addition to administrative penalties and other administrative measures as well as administrative fines, Member States must ensure that their competent authorities have the power to impose, in the event of an infringement of the own funds requirement of art. 67 MiCAR, to impose a temporary ban preventing any member of the management body of the CASP, or any other natural person who is held responsible for the infringement, from exercising management functions in a CASP.[102]

In our experience, the stipulations that need to be included in terms of a CET1 issue, e.g. in the articles of association or the shareholder's agreements, are often not in line with the existing capital structures of CASPs. We therefore recommend prospective CASPs to engage in a timely discussion with their shareholders and competent authorities to ensure that the required adjustments have been made in order to have sufficient regulatory capital.

Contrary to investment firms, no internal risk assessment procedure such as the ICARAP or ICLAAP exists, with equally no supervisory review and evaluation process (SREP) process being undertaken by the competent authorities. In principle, CASPs are therefore only subject to Pillar 1 and 3 requirements with, as it seems now, no possibility for a competent authority to impose an additional Pillar 2 capital requirement.

[100] As these in tokenized form would be subject to the MiFID II regime, being security tokens.

[101] Art. 3 Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included in a notification by certain financial undertakings of their intention to provide crypto-asset services.

[102] Art. 111(4) MiCAR.

6. QUALIFYING HOLDINGS

6. QUALIFYING HOLDINGS

Similar to certain other financial undertakings, the acquisition of a qualifying holding in a CASP (i.e., a direct or indirect holding in the CASP which represents at least 10% of the capital or voting rights), is subject to a regulatory approval regime.[103] The competent authority for the approval of acquisitions of qualifying holdings in Dutch financial undertakings is DNB or the ECB.

During the course of an application for approval, DNB tests the suitability and financial soundness of the acquirer against the following criteria:

I reputation of the acquirer;

II reputation, knowledge, skills and experience of any person who will direct the business of the CASP as a result of the proposed acquisition;

III financial soundness of the acquirer;

continued regulatory compliance;

IV AML/CTF factors.

The supervisor must conduct its assessment strictly in accordance with MiCAR, being a Regulation, and not its national regime, which could result in minor differences between existing (national) qualifying holding regimes and the MiCAR qualifying holding regime. Nevertheless, these national regimes are predominantly based on EU legislation (e.g., CRD IV, PSD2 or MiFID II) and closely align with the requirements under MiCAR. ESMA has further drafted RTS setting out the details of the approval application,[104] in which it sought connection to the existing guidance on the topic of qualifying holdings in the financial sector.[105] Depending on the size of the qualifying holding, the level of information requested may be more or less intensive, with the largest burden for prospective acquirers intending to hold the CASP as a (wholly-owned) subsidiary.

[103] Art. 83 MiCAR.

[104] Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation EU (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content of the information necessary to carry out the assessment of the proposed acquisition of a qualifying holding in a CASP.

[105] ESA, Joint Guidelines on the prudential assessment of acquisitions and increases of qualifying holdings in the financial sector, (2016).

7. SAFEGUARDING OF CLIENT CRYPTO-ASSETS

7. SAFEGUARDING OF CLIENT CRYPTO-ASSETS

CASPs are required to have adequate arrangements to safeguard the ownership rights of clients and to prevent the use of clients' crypto-assets for their own account.[106] The strict requirements that are being introduced regarding the safekeeping of customer assets can be directly connected to the recent incidents regarding the protection of customer ownership rights as a result of the failures of Celsius, Voyager and FTX.

CASPs may opt to also offer clients custody and administration of crypto-assets, where applicable in the form of private cryptographic keys[107], or to use the custody services of another CASP. These services are also known as the offering of custodian wallets.[108]

7.1 Safeguarding arrangements

CASPs offering custodial wallets need to ensure that adequate arrangements for the safeguarding of the ownership rights of the clients with respect to the crypto-assets held on their behalf are in place, creating a bankruptcy remote perimeter around the safeguarded assets.[109] Moreover, where CASPs hold clients' funds other than e-money tokens, they must design proper arrangements that prevent the CASP from using those funds for own account. Such funds must be deposited with a bank or central bank before the end of the day on the business day following on which the CASP received the funds. Such safeguarding account needs to be separately identifiable from the CAPS's account.

[106] Art. 70(1) MiCAR. The AFM has indicated that it does not intend to goldplate the custody requirements for CASPs, thus staying true to the wording of MiCAR without imposing additional requirements.

[107] Art. 3(1)(17) and 75 MiCAR.

[108] Recital (83) MiCAR states that hardware or software providers of non-custodial wallets are not covered by the scope of MiCAR.

[109] Art. 70(1) MiCAR.

The safeguarding policy of a CASP must specify the following items[110]:

I how the CASP ensures that: (i) clients' funds are not used for its own account; (ii) crypto-assets belonging to the clients are not used for its own account without the clients' explicit consent; and (iii) the addresses of clients' crypto wallets are different from the notifying entity's own wallet address;

II a detailed description of the approval system for cryptographic keys and safeguarding of cryptographic keys (for instance, multi-signature wallets);

III how the CASP segregates clients' crypto-assets;

IV a description of the procedure to ensure that clients' funds are deposited with a (central) bank in a timely manner;

V which factors the CASP is taking into account to select the bank to deposit clients' funds, including the notifying entity's diversification policy;

VI how the CASP ensures that clients are informed in clear, concise and nontechnical language about the key aspects of the safeguarding arrangements of the CASP.

7.2 Custody policy

A CASP that offers the custody and administration service must conclude a written contract governing the custody relation.[111] In that agreement: (a) the identity of the parties to the agreement needs to be stated[112]; (b) the nature of the crypto-asset service provided needs to be described in addition to a description of that service, where a mere copy of the MiCAR definition will most likely not suffice; (c) the custody policy of the CASP must be shared; (d) the means of communication between the CASP and the customer, including the customer's authentication system needs to be described; (e) a description of the security systems used by the CASP must be

[110] Art. 5 Commission Delegated Regulation (EU) 2024/XXX of XXXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the information to be included in a notification by certain financial undertakings of their intention to provide crypto-asset services.

[111] Art. 75(1) MiCAR. This agreement may be standardised.

[112] Whereby the use of other parties, being CASPs pursuant to art. 59 MiCAR, shall be notified to the client pursuant to art. 75(9) MiCAR.

included; (f) the fees, costs and charges applied of the service must be clarified;[113] and (g) the applicable law governing the agreement needs to be specified.[114]

CASPs must in any case ensure that, when safeguarding crypto-assets on behalf of clients, the client's rights that are attached to the crypto-assets can be exercised, including in cases where the underlying rights of the crypto-assets change.[115] At least every three months the CASP must provide its clients with an electronic statement of their position of crypto-assets, wherein the crypto-assets concerned are identified, their balance, their value and the transfer of crypto-assets made since the last report.[116] Moreover, if need be, the CASP must be able to return the crypto-assets to the client as swiftly as possible, for which procedures need to be included in the custody policy.[117]

Taken together, the custody policy minimises the risk of loss of clients' crypto-assets or the rights related to those crypto-assets or the means of access to the crypto-assets due to fraud, cyber threats, negligence or bankruptcy.[118] Although the custody policy is relatively comprehensive, the CASP must share a summary of the custody policy with the client at their request.[119]

Perhaps the most interesting about the safeguarding requirements is the obligation for the CASP to technologically segregate the crypto-assets held on behalf of their clients from their own crypto-assets on two or more distinct DLT addresses, ensuring that the means of access to crypto-assets of their clients is clearly identified as such.[120] The crypto-assets held in custody by a CASP must be legally segregated from the CASP's estate in the interest of its clients in accordance with applicable law.[121] By doing so, creditors of the CASP have no recourse to

[113] Interestingly enough, where the requirement of informing the client on all relevant costs and charges is a general obligation under MiFID II, particularly art. 24(4) thereof and as detailed in art. 50 DR MiFID II, MiCAR chooses to include this disclosure requirement in an article specific to the custody service. Whether its contents must be extrapolated to other crypto-asset services that are provided by the CASP in question is unclear, but also not impossible under the current wording, although this would seemingly be contrary to the approach of including costs disclosure requirements in respect of specific services, as also is specifically required for CASPS offering advisory services pursuant to art. 81(4) MiCAR. MiCAR does require the policies on costs, pricing and fees to be publicly available on the CASP's website, pursuant to art. 66(4) MiCAR.

[114] Art. 75(1) MiCAR; which may make a significant difference based on the applicable property law principles, for instance those surrounding the legal phenomenon of comingling. These requirement are closely aligned with, but not identical to, those included for client asset separation under MiFID II; Art. 24(4) MiFID II and art. 49 DR MiFID II.

[115] Art. 75(4) MiCAR; This provision might have a significant impact in future insolvency cases as it probably can be construed to have a direct effect, being a sufficiently clear and precise provision of an EU Regulation that seeks to award a certain right to clients.

[116] Art. 75(5) MiCAR.

[117] Art. 75(6) MiCAR.

[118] Art. 75(3) MiCAR.

[119] Ibid.

[120] Art. 75(7) MiCAR; Thus, whilst omnibus DLT addresses might be acceptable for the holding of client crypto-assets they cannot comingle with the crypto-assets of the CASP itself, which means that it must utilise its own separate DLT address.

[121] It remains to be seen how this segregation will be implemented in practice.

crypto-assets held in custody by the CASP, in particular in the event of insolvency proceedings. In the event of a loss of client crypto-assets, the CASP will be liable for an amount equal to the market value of the lost assets, insofar the incident causing the loss is attributable to the CASP.[122] CASPs using permissionless DLT infrastructure that they do not control or manage, i.e., where no contractual arrangement exists, are probably exempted from this liability.[123]

[122] Art. 75(8) MiCAR.

[123] ESMA, 2023b, paragraph 62.

8. RECORD-KEEPING AND REPORTING

8. RECORD-KEEPING AND REPORTING

Similar to the requirements applicable to investment firms under MiFIR[124], CASPs (particularly those operating trading platforms) are subject to pre- and post-trade transparency requirements under MiCAR.[125] The main difference between the two (2) regimes is, however, that transparency is one of the inherent features of DLT and arguably its main selling point. Therefore, MiCAR is far less comprehensive and prescribing when it comes to transparency requirements than MiFIR. This is exemplified by the fact that the transparency requirements under MiCAR will be transposed through an RTS whereas MiFIR is a Level 1 Regulation.

8.1 Pre-trade transparency

CASPs operating a (centralised) trading platform are required to publish bid and ask prices and depth of interest with regards to any crypto-asset traded on their platform on a continuous and real-time basis during trading hours.[126] No exemptions with regards to the pre-trade transparency regime exists in the MiCAR, contrary to the complicated landscape of MiFIR. That means that for instance large (block) trades are also subject to pre-trade transparency requirements under MiCAR contrary to the exceptions in MiFIR.

8.2 Post-trade transparency

Under MiCAR, CASPs operating a trading platform will be held to publish post-trade transparency data as close to real-time as is technically possible and in any case within 30 seconds of the relevant transaction.[127] This is a significantly shorter timeframe than under MiFIR. The difference has been rationalised by ESMA because of the speed with which transactions are processed on the average blockchain. ESMA understands there are various blockchain network speeds in terms of the average time it takes for a block to be added to the relevant blockchain. Nevertheless, ESMA considers that for centralised exchanges, block times should

[124] Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

[125] Art. 76(9) MiCAR.

[126] Ibid.

[127] Article 4 of Commission Delegated Regulation (EU) 2024/XXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the manners in which transparency data for CASPs operating a trading platform for crypto-assets is to be presented.

not be taken into account since the post-trade requirements for crypto-asset platforms apply when the transaction is agreed on the trading platform, which moment does not typically coincide with the registration on the blockchain.

8.3 Record-keeping

Pursuant to MiCAR, CASPs must maintain records of all crypto-asset services, activities, orders and transactions undertaken by them,[128] and provide such records to competent authorities and clients upon request.[129] This requirement has been further detailed in a (draft) RTS and is based on MiFID II RTS 22[130] and 24[131]. No fixed reporting time (e.g., T+1) is set by MiCAR nor does MiCAR provide for a transaction reporting obligation.[132] Therefore, the data reported in accordance with art. 68(9) MiCAR will be the only transaction data available to the supervisory authorities. The data fields that must be recorded are defined in two (2) RTS, one (1) for all CASPs and one (1) for CASPs operating a trading platform.[133] The recorded data must be maintained for a period of five (5) years and, where requested by the competent authority before such five (5) years have elapsed, for a period of up to seven (7) years.[134]

[128] Where undertaking a transaction means executing a conclusion of an acquisition or disposal of a crypto-asset or transmitting an order.

[129] Art. 68(9) MiCAR.

[130] Commission Delegated Regulation of 28 July 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the reporting of transactions to competent authorities.

[131] Commission Delegated Regulation (EU) 2017/580 of 24 June 2016 supplementing Regulation (EU) No 600/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the maintenance of relevant data relating to orders in financial instruments.

[132] Art. 26 MiFIR.

[133] Commission Delegated Regulation (EU) …/… of XXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying the content and format of order book records for CASPs operating a trading platform for crypto-assets.

[134] Art. 4 Commission Delegated Regulation (EU) 2024/… of XXX supplementing Regulation (EU) 2023/1114 of the European Parliament and of the Council with regard to regulatory technical standards specifying records to be kept of all crypto-asset services, activities, orders and transactions undertaken.

9.
REQUIREMENTS APPLICABLE TO THE NOTIFICATION REGIME

9. REQUIREMENTS APPLICABLE TO THE NOTIFICATION REGIME

In order to use the notification regime (as set out in Section 3.3), regulated financial undertakings must notify the AFM[135], regardless of whether the entity in question obtained its licence from the AFM, of the following information:[136]

I a programme of operations setting out the types of crypto-asset services that the undertaking intends to provide, including where and how those services are to be marketed;

II a description of:

- a the internal control mechanisms, policies and procedures to ensure compliance with the applicable AML/CTF framework, i.e. the AML/CTF policy adapted for crypto-asset services;
- b the risk assessment framework for the management of ML/TF risks, i.e. the SIRA adapted for crypto-services;
- c the business continuity plan;

III the technical documentation of the ICT systems and security arrangements, and a description thereof in nontechnical language;

IV a description of the procedure for the segregation of clients' crypto-assets and funds;

V a description of the custody and administration policy, where it is intended to provide custody and administration of crypto assets on behalf of clients;

VI a description of the operating rules of the trading platform and of the procedures and system to detect market abuse, where it is intended to operate a trading platform for crypto assets;

VII a description of the non-discriminatory commercial policy governing the relationship with clients as well as a description of the methodology for determining the price of the crypto-assets they propose to exchange for funds or other crypto-assets, where it is intended to exchange crypto-assets for funds or other crypto assets;

[135] The implementing Dutch regulation specifying the competent authorities in accordance with art. 93 MiCAR makes the somewhat difficult decision to appoint the AFM as the first point of contact for both authorisation applications and notifications by financial undertakings. This means that, for instance, a credit institution must notify the AFM of its intent to start providing crypto-asset services, who will then, presumably, contact DNB (or the ECB) to verify what information is already there. An interesting question could be to what extent the AFM is free to form a judgment over existing documentation, e.g., can it deviate from a supervisory judgment from DNB or the ECB?

[136] Art. 60(7) MiCAR and as further to be detailed in an RTS as published for consultation by ESMA.

VIII a description of the execution policy, where it is intended to execute orders for crypto assets on behalf of clients;

IX evidence that the natural persons giving advice on behalf of the applicant CASP or managing portfolios on behalf of the applicant CASP have the necessary knowledge and expertise to fulfil their obligations, where it is intended to provide advice on crypto-assets or provide portfolio management on crypto assets;

X whether the crypto-asset service relates to asset-referenced tokens, e-money tokens or other crypto assets;

XI information on the manner in which transfer services will be provided, where it is intended to provide transfer services for crypto assets on behalf of clients.

Notifying financial undertakings will be exempted from the full authorisation requirements[137], prudential requirements (Section 5)[138], and the qualifying holdings regime (Section 6).[139] Interestingly, that means that notifying financial undertakings remain, in principle, subject to the requirement under MiCAR of the passporting regime,[140] the obligation to act honestly, fairly and professionally in the best interest of clients,[141] the governance arrangements[142] and all service-specific requirements.[143]

In order to satisfy the requirements applicable to the notification regime, we expect that notifying financial undertakings must, at a minimum, thoroughly revise their custody and ICT policies and programmes of operations, at least in respect of the crypto-asset services they wish to provide. Other policies may, depending on the concrete facts and circumstances of the case, potentially be submitted with limited alterations.

[137] Art. 62 and 63 MiCAR.

[138] Art. 67 MiCAR. financial undertakings remain subject to their own prudential framework (e.g., IFR, CRR).

[139] Art. 83 and 84 MiCAR.

[140] Art. 65 MiCAR.

[141] Art. 66 MiCAR.

[142] Art. 68 MiCAR, see paragraph 4.

[143] Art. 70 et seq. MiCAR.

Whilst it may be a logical expansion for some financial undertakings to provide crypto-asset services, we identify that due to the fact that crypto-assets will be subject to a *sui regime*, i.e. MiCAR, the supervisors may reasonably expect that a board member (e.g., of a bank or investment firm) has (some) knowledge of crypto-assets. In particular, we wonder to what extent the supervisors deem a rescreening in order when a financial entity expands its services to the crypto-sphere. Should existing board members be assessed for their fitness at the occasion of notification (see Section 3.3)? Moreover, would it be possible that an established – say bank – which has expanded its services to crypto-assets and subsequently wishes to appoint a new board member may be faced with a negative supervisory assessment if that board member has no knowledge of crypto-assets even though he may be vastly experienced in the 'regular' banking sphere? We do not directly expect such issues to materialise for larger institutions whose activities predominantly consist of conventional financial services nor for other institutions generally. However, it remains imperative that the board of a financial entity, including CASPs, is sufficiently in control and thus possesses an adequate level of crypto-asset knowledge.

****