DARTE SERIES

Madrid 2.0

Initiated by Dr. Nina-Luisa Siedler (siedler legal) and Mariana de la Roche W. (BlackVogel), the DARTE Series aims to enhance legal clarity within the evolving regulatory framework of the EU MiCAR. Over time, the series has expanded to address adjacent regulatory regimes, jurisdictional divergences, and emerging technological challenges shaping the crypto-asset ecosystem in Europe.

The Madrid 2.0 DARTE edition was held on October 7th, 2025, at the historic Palacio de Santoña, in collaboration with the European Commission, Project Catalyst, MERGE Madrid, Sumsub, and TRM Labs. The session brought together regulators, legal experts, compliance professionals, and industry innovators to engage in high-level dialogue around operationalizing MiCAR across borders, safeguarding crypto markets from abuse, and exploring novel asset structures such as liquid staking tokens.

Discussions centered on three key topics: cross-border implementation challenges of KYC/AML frameworks under MiCAR (Katherine Cloud, Sumsub), the evolving enforcement landscape around market abuse in crypto-assets (Luiza Castro Rey, TRM Labs), and a practical case study on tokenizing liquid staking mechanisms in a compliant way (Juan Ignacio Ibañez, MiCA Crypto Alliance). The roundtable opened with keynote remarks from Dr. Joachim Schwerin (European Commission) and Jacob Cohen (TRM Labs), who emphasized the growing importance of transatlantic cooperation, responsible innovation, and supervisory clarity as the sector matures.

We extend our sincere thanks to all speakers, contributors, and institutional partners for their generous support in making this roundtable possible. This report captures the insights shared during the session. The views presented reflect the collective understanding of the participants and do not necessarily represent the positions of individual attendees or rapporteurs.

1. **Cross-Border Implementation of MiCAR KYC/AML Standards**

The first topic, introduced by Katherine Cloud (Sumsub), examined the significant operational and legal challenges faced by CASPs in complying with MiCAR's KYC and AML standards across multiple EU jurisdictions. While MiCAR aims to harmonize crypto regulation within the European Union, real-world implementation is complicated by varying national laws, document types, identity verification procedures, and privacy rules.

Participants emphasized that CASPs with cross-border operations must navigate a patchwork of legal expectations that can delay onboarding, increase compliance costs, and heighten regulatory risk. Manual processes for identity verification and risk monitoring, still common in many jurisdictions, are prone to human error and create inconsistent user experiences. This inconsistency directly undermines MiCAR's goals of consumer protection, financial integrity, and regulatory oversight.

The discussion highlighted the potential of advanced technology, including AI-powered document checks, biometric matching, and dynamic risk-scoring models, to streamline compliance. However, without a recognized pan-European framework for digital onboarding and ongoing monitoring, CASPs face uncertainty over what counts as "adequate" under MiCAR.

A flexible but structured framework that could serve as a blueprint for both regulators and market participants was proposed. The model would emphasize transparency, auditability, and proportionality, defining minimum compliance expectations without imposing one-size-fits-all technical mandates. A key proposal was the creation of an expert working group that includes regulators, regtech firms, and EU institutions to map divergences and promote interoperability across Member States.

An illustrative example discussed involved RegTech providers reporting suspicious transactions directly to authorities on behalf of CASPs through secure APIs. This would help reduce operational burdens while ensuring traceability and regulatory alignment. Several participants also noted the need to ensure proportionality for smaller actors and startups, ensuring they can comply without incurring prohibitive costs.

Participants welcomed the notion that MiCAR compliance should be principle-based rather than driven by rigid templates. In particular, a risk-based and adaptive framework could better align with both the fast-moving innovation cycles in crypto and the varying maturity levels of compliance infrastructure across Europe.

Call to Actions regarding MiCAR KYC/AML Implementation

The key call to actions from the discussion are:

- **Establish a cross-border compliance coordination group:** Regulators, market actors, and regtech providers should jointly form an expert working group to develop common frameworks for identity verification, ongoing monitoring, and suspicious activity reporting, adapted to national differences but aligned with MiCAR's core principles.

- **Promote interoperable, principle-based technical guidelines:** Instead of rigid reporting templates, the industry should define adaptive technical and legal standards - such as secure APIs for RegTech integration—that ensure transparency, auditability, and proportionality in both onboarding and risk monitoring.

2. Prevention and Prohibition of Market Abuse Involving Crypto-Assets

The second topic, introduced by Luiza Castro Rey, addressed the urgent need for clearer operational standards and compliance tools under MiCAR Title VI, which came into full application on December 30, 2024, for all Persons Professionally Arranging or Executing Transactions (PPAETs). Participants focused on the structural challenges of preventing and detecting market abuse in the unique context of crypto markets - challenges that differ significantly from those in traditional finance.

Crypto markets are structurally complex: trading is continuous (24/7), assets are listed on hundreds of platforms, and prices vary widely across centralized and decentralized venues. Manipulative behavior takes on new forms, from pump-and-dump schemes to oracle exploits and cross-venue arbitrage strategies. While vast amounts of on-chain data are technically transparent, most actual trading still occurs off-chain, on opaque, centralized platforms, complicating surveillance. Additionally, pseudonymity and fragmented identities make it difficult to identify connected persons or employees engaged in insider dealing.

Participants expressed concern that MiCAR and its accompanying ESMA RTS fail to offer practical guidance on what "sufficient internal controls" should look like. Compliance teams are left to interpret broad obligations without clarity on how to approach:

- Employee wallet declarations.
- Surveillance across off-chain and cross-chain behavior.

- Balancing privacy laws with monitoring obligations.
- Distinguishing between material non-public information and publicly available on-chain data.

Another key discussion point was the definition of "inside information" in the crypto context. MiCAR borrows core principles from the Market Abuse Regulation (MAR) but implements them in a lighter form, particularly not requiring issuers from MAR-style insider lists. This is meant to ease the burden on SMEs and the still native crypto market. However, as soon as a crypto asset becomes underlying to a financial instrument (like derivative, ETN) the more comprehensive MAR market manipulation rules apply again. Participants also debated whether vulnerabilities in smart contracts, DAO governance proposals, or upcoming protocol upgrades qualify as inside information, especially when disclosed on-chain but not widely understood or flagged to the broader public.

Participants agreed that in the absence of consistent enforcement approaches across the EU, both compliance effectiveness and legal certainty are at risk. The roundtable called for structured dialogue with ESMA and national regulators to align on expectations and create crypto-specific adaptations of traditional market abuse controls.

Call to Actions regarding Market Abuse in Crypto Markets

The key call to actions from the discussion are:

- **Establish an industry-led insider dealing compliance taskforce:** Convene regulators, CASPs, and legal experts to develop realistic, proportionate best practices tailored to crypto markets - such as employee wallet frameworks, modified insider lists, and cross-chain surveillance protocols.

- **Clarify the definition of inside information for crypto-assets:** Align market understanding through regulatory Q&A and joint guidance, focusing on the treatment of on-chain disclosures, protocol vulnerabilities, and crypto-specific materiality thresholds, with scaled obligations for SMEs.

Launch of the Tokenization of Liquid Staking taxonomy.

Following the above expert discussions, the final presentation of the Madrid 2.0 DARTE session revisited a key topic that first emerged during the Vienna 2.0 roundtable: The classification challenges of decentralized assets, with Liquid Staking Tokens (LSTs) serving as a central case study. Building on those earlier discussions, the Liquid Staking Tokenization (LST) Project was presented as a concrete next step toward resolving regulatory ambiguity in this area.

LSTs represent a growing category of crypto-assets that allow users to retain liquidity while staking assets like ETH. However, they do not neatly fit into MiCAR's core classifications of utility tokens, ART or e-money tokens - due to the absence of identifiable issuers, claimable returns, or redemption mechanisms. Their decentralized nature and protocol-level governance further complicate their treatment under MiFID II or AIFMD.

To address this gap, the project proposes a dedicated taxonomy based on objective indicators such as decentralization, economic design, and technical risks. It also explores how the MiCAR whitepaper obligations could be adapted when no legal issuer exists, suggesting that the listing CASP could assume disclosure responsibilities focused on smart contract audits and risk transparency.

This project aims to support regulatory convergence, reduce liability risk for CASPs, and enable the safe and compliant offering of LSTs in the EU. It reflects the broader DARTE objective of facilitating industry-led solutions in cooperation with policymakers.

Please find the one-pager summarizing the LST Tokenization Project here.

We thank all participants of the Madrid 2.0 DARTE event for contributing to the discussion:

Adela Pizarro, Almudena de la Mata (Blockchain Intelligence), Andrea Disaro (DeFi Technologies), Andrew Stakiwicz (Hashgraph), Asa Dahlborn (BlackVogel), Ben Bowden (Binance), Claudia Sotelo (CMF), Dennis Rasch (Golem Foundation), Dmitrij Uskov (Bybit), Eric Piscini (Hashgraph), Fernando Zornig (Sumsub), Gabriel Campa (TowerBank), Hannah Zacharias (21Analytics), Jacob Cohen (TRM Labs), Jaime Pradenas (Banco Central Chile), Joachim Schwerin (European Commission), Juan Carlos Reyes (CNAD), Juan Eugenio Tordesillas (ECIJA), Juan Ignacio Ibanez (MiCA Crypto Alliance), Katherine Cloud (Sumsub), Lola Noguera (Binance), Lucia Suarez (Santander), Luiza Castro Rey (FiO Legal), Manu Fernandez (TRM Labs), Mariana de la Roche (BlackVogel), Mariona Pericas (finReg360), Marta Chavarria (SEG Social), Nicole Dyksant (TaxBit), Nil Daunis (Sumsub), Nina-Luisa Siedler (siedler legal), Pedro Mendez de Vigo (Crypto.com), Rocio Alvarez-Ossorio, Sonia Salvatierra (CNV Argentina), and Thomas Taranikuk (Sumsub).