DARTE SERIES

Madrid 3.0

Initiated by Mariana de la Roche W. (BlackVogel) and Dr. Nina-Luisa Siedler (siedler legal), the DARTE Series is a high-level roundtable format designed to enhance legal clarity around digital assets, focusing on regulation, compliance, data protection, and market integrity.

The Madrid 3.0 DARTE edition took place on 27 October 2026 in Madrid, in collaboration with CertiK, ISBE, MERGE and MÖHRLE HAPP LUTHER.

The agenda focused on three themes: 1) crypto-native incident classification under DORA, presented by Jason Jiang 2) DAC8 and standardised asset identifiers, presented by Marie Christin Rinke, and 3) CASP and PSP partnership models under MiCAR and PSD2/PSD3, presented by Marina Villalonga.

A theme that ran through all three discussions was the cost of extending frameworks built for traditional finance onto crypto-asset activity without adapting their categories. In each case the friction was the same: the classifications do not map onto on-chain events, the reporting demand is produced but cannot be used for its stated purpose, and the market is left to construct compliant structures without a template from the supervisor.

We extend our sincere thanks to all speakers, participants, and institutional partners for their valuable contributions. The views presented in this report reflect the collective understanding of the participants and do not necessarily represent the official positions of individual attendees or the rapporteur.



Opening Keynote.

The session opened with a keynote by Miguel Ángel Calero, Executive Director of ISBE at Alastria.

The keynote focused on three vectors of friction that arise in Europe when regulated actors use permissionless blockchains. The first is operational resilience: who is accountable for the infrastructure, what the business continuity plan is, who the validators are and, since DLT networks are an IT system, who operates it and bears responsibility for it. The second is the GDPR, described as a European concern that becomes concrete the moment a person's own data is written on chain. The third is technological sovereignty: the conclusion reached in 2022 that all software should be open source and that all computing power should be located in European territory and subject to European jurisdiction.

The keynote then set out how each friction had been addressed in ISBE, a blockchain services infrastructure built in Spain and intended to operate at European level, developed on the basis of existing regulation and standards and on requirements gathered from the public sector and regulated industries. On resilience, a single operator holds all liability, at present Alastria; validator nodes, identified and run by public bodies, large companies, universities, research centres and qualified trust service providers, are being added in Spain, Germany, France, Italy, the Netherlands and Belgium; and transaction finality is immediate, with fixed block times. Every company operating on the network is also identified through a qualified X.509 certificate of its legal representative (LEAR), an arrangement acknowledged to raise confidentiality questions of its own, and one expected to arise on permissionless chains as well. On data protection, a confidentiality layer prevents participants from viewing each other's transactions while preserving access for regulators, a solution noted as probably not suited to permissionless networks; a filtering proxy allows accounts, transactions or operations to be hidden where an operator has written personal data in plain text; and a kill switch exists for every account and smart contract, reflecting requirements raised by banks and European institutions.

The keynote closed with the observation that ISBE had been built from regulatory requirements outward, and that the result supports programmable identity and programmable processes alongside programmable money, for the financial sector and beyond. Several of the questions raised were noted as returning later in the session.

1. Crypto-native incident classification under DORA

The first topic, presented by Jason Jiang, Chief Business Officer at CertiK, addressed the application of DORA's incident regime to crypto-asset activity, specifically the definition of an ICT-related incident in Article 3(8) and the management, classification and reporting obligations in Articles 17 to 20. The presentation framed these provisions as drafted for ICT systems under the regulated entity's own control, with crypto-asset activity producing boundary cases the regime does not anticipate. An external protocol exploit must be assessed as to whether it is an incident at all; a market loss or the impact of a stablecoin depeg does not automatically constitute

an ICT incident; and the thresholds and timelines assume facts that are hard to establish on chain.

Four difficulties were set out. First, affected clients and services are hard to define, because crypto-assets are adopted worldwide and automated on-chain assessment is difficult to make accurate. Second, integrity can be compromised without any downtime: a signing-key compromise, oracle manipulation or bridge exploit can affect the integrity of a whole chain while availability is unaffected, so availability-based triggers miss the event, and commercial loss can occur without any service interruption. Third, timing: a block timestamp may precede both the entity's awareness and its documentation of the event, and the position presented was that public visibility on chain should not automatically be treated as awareness for the purposes of the reporting clock. Fourth, losses and recovery are hard to quantify, especially on a gross basis, and confidence in attribution and the recovery position change over time in ways that alter the classification.

The solution presented was a proportionate, crypto-native incident classification under DORA, applied to the existing threshold forms and deadlines, with a shared interpretation of what constitutes an incident in this context. The presentation pointed to regimes that already carry more technically detailed requirements, including ADGM, the Hong Kong SFC and NIST in the United States, and included an offer to share ADGM's classifications as a reference. The proposed minimum data set for a crypto-native incident report comprises block timestamps, the first alert, documented awareness, classification and any reclassification, chain and transaction references, impacted services and clients, the integrity or availability effects, and the methodology used to quantify loss or exposure.

The discussion that followed confirmed that the problem is real but early. Firms are only beginning to integrate DORA, and no reporting template has come from the regulator, which participants expected to produce reports that differ substantially from one another, make the supervisor's work harder, and push entities toward over-reporting for fear of falling short. Defining the minimums of a report was identified as the priority.

A central thread concerned awareness and the start of the reporting clock. The view reached in the series' earlier market-abuse discussion was reiterated: what is publicly visible on chain counts as known, or as something that should have been known, and participants did not expect supervisors to accept otherwise. The counterpoint drew a line between layers. The bare facts readable on the chain are public; the attribution of a wallet to a person or entity, and off-chain analysis available only to paying customers of an analytics provider, are proprietary and should not be treated as public knowledge. The practical question is therefore what triggers the four-hour and 24-hour notification windows: on-chain data alone cannot populate DORA's categories, and the analysis required to do so takes time. Participants with operational experience noted that an exploit can be identified on chain within minutes to an hour, that establishing the root cause takes at least several hours, and that sizing the full loss of a major exploit took at least a day in recent cases, by which point the European deadline has

passed. The compromise proposed was to report that an incident has occurred as soon as it is detected, with the root-cause investigation continuing after the initial notification.

A related exchange concerned blockchain analytics. The call for providers to align their methodologies, raised in earlier DARTE sessions, was rejected by those with provider experience: clustering and attribution approaches differ fundamentally, the rigour behind them is costly and competitively valuable, and some outputs are demonstrably better than others, as shown by error rates and admissibility in court. What participants supported instead was disclosure of methodology, so that reports are explainable and comparable, together with minimum quality benchmarks. The open wallet attribution initiative of the Global Coalition to Fight Financial Crime was noted as one response to the comparability problem. Participants also distinguished on-chain data providers from attribution providers, observing that the real issue lies with how the obliged entity categorises the information it receives from both.

Two further points shaped the solution. The first was record-keeping: because incidents evolve, authorities want an internal record, beyond the report, of who knew what, at what time, and what was decided, traceable to the individuals involved, and participants agreed this should be tamper-proof. A parallel was drawn with sanctions-list enrichment, where reporting deadlines were in practice pushed back onto data providers through contractual service levels; the same mechanism applies here. The second was monitoring. Tools exist that detect exploit characteristics across smart contracts in near real time, and participants, including those sceptical of regulatory expansion, considered an on-chain monitoring obligation for CASPs relying on smart contracts to be justified, because detection serves consumer protection before it serves reporting. The cost for small and mid-sized CASPs was raised as a proportionality concern, with the observation that regulators worldwide are raising the operational bar for CASPs.

The discussion of attribution surfaced a disagreement on identity. One view held that if Europe is moving to atomic settlement it must also move to atomic identity, connecting on-chain and off-chain identity for legal persons through mechanisms such as the T-REX token standard, ISO 24165 identifiers and trust and service registries, with a permissioned layer over permissionless infrastructure where necessary. This was resisted on two grounds: that permissioning permissionless networks removes what the technology is meant to provide, and that concentrating identity data creates honeypots. The distinction between natural persons, whose privacy is protected, and legal persons, which have no comparable privacy right, narrowed the disagreement, as did the observation that DORA concerns regulated entities that already hold the data needed for attribution. Participants noted that ICT third-party providers are not necessarily CASPs, so any taxonomy must cover both. The closing contributions pointed to ESMA's common supervisory action on DORA in the crypto sector, focused on custody risks and running to the second half of 2027, as the channel through which a classification proposal should be fed, and flagged the Cyber Resilience Act as a parallel regime shifting the perspective to

the regulated entity's customers and not fully aligned with DORA.

Calls to Action regarding DORA incident classification

The key calls to action from the discussion are:

- **Compare incident classification regimes and extract the minimums:** the trade associations represented should undertake a comparative study of ADGM, the Hong Kong SFC, NIST and comparable regimes, identify the minimum categories and data fields they require, and propose a crypto-native classification for DORA built on those minimums.
- **Agree a common taxonomy of events between CASPs and ICT third-party providers:** obliged entities and their ICT providers, including providers that are not CASPs, need a homogeneous categorisation of the events that can arise in their interaction and of how each is treated for reporting; this taxonomy should be submitted to ESMA's common supervisory action on custody before it concludes in 2027.
- **Define the awareness trigger in layers:** bare on-chain facts count as known; proprietary attribution and paid off-chain analysis do not; the notification clock runs from detection that an incident has occurred, with root-cause analysis and loss quantification following in subsequent updates.
- **Require a tamper-proof record of awareness and decisions:** entities should maintain an internal record of who knew what, when, and what was decided, built on existing disclosure-record processes, so that evolving incidents can be traced to the individuals who acted on them.
- **Introduce a proportionate on-chain monitoring obligation:** CASPs relying on smart contracts should be expected to run continuous on-chain monitoring for exploit characteristics, framed as consumer protection, with proportionality for small and mid-sized entities that cannot maintain their own investigations function.
- **Replace methodology harmonisation with methodology disclosure:** analytics providers should not be asked to align clustering and attribution methods; they should disclose them, and a set of minimum quality benchmarks should allow customers and courts to compare outputs.

2. DAC8 and standardised asset identifiers

The second topic presented by Marie Christin Rinke, Partner at MÖHRLE HAPP LUTHER, returned to DAC8, which the series had previously examined in Vienna, and addressed the gap between what the framework collects and what it can achieve.

The problem was set out through a concrete case. A taxpayer holding wallets at several CASPs files a tax return using a crypto tax tool. Each CASP separately reports under DAC8 on the assets it holds or custodies for that person, without coordination with the others. What each treats as a taxable event differs from what the taxpayer treats as one: the wrapping or bridging of a token may not be a taxable event in the taxpayer's own records however under DAC8 still appear as a potentially taxable sale; unsolicited spam and scam tokens pollute wallet data and are hard to separate from genuine holdings; and the same asset may be reported under different names by different reporters. The tax authority therefore receives several reports on the same person that do not match, and cannot tell which asset is being moved. CASPs report aggregated data that cannot be used to calculate tax, while the taxpayer receives only the CASP's transaction files, not the DAC8 report itself. Participants added a structural point: tax is national and DAC8 reporting is transnational, so a report meaningful in every jurisdiction is technically not possible. They also raised proportionality: an infringement of privacy must be proportionate and achieve its purpose, and data collection that serves no usable purpose fails that test.

The first proposal, and the one the session concentrated on, was a single standardised asset identifier used consistently by every reporting party, so that the same asset carries the same name respectively unique identification everywhere and i. e. a token wrapping an asset is distinguishable from the asset itself. The existing standard is the Digital Token Identifier under ISO 24165, administered by the Digital Token Identifier Foundation. The second and third proposals were not reached and were deferred to a subsequent session.

The discussion focused on three questions. The first was the purpose of the regime. If the aim is to detect evasion, participants suggested the necessary information is far narrower: which persons hold wallets where, and whether they filed. Reporting every transaction produces data nobody can use; reporting aggregates produces data nobody can calculate tax from. One route is for the CASP to understand what constitutes a taxable event in the taxpayer's jurisdiction and report only that, which shifts a substantial burden onto the CASP. Another is to agree in advance which technical events, such as a wrap or a bridge, entail an economic change and which do not, so that tax concepts can be layered onto a shared technical classification. Participants were uncertain whether such scenarios can be defined given the variety of bridging and staking mechanisms, but agreed the attempt is worthwhile.

The second question was the identifier itself. Naming by exchange symbols fails because symbols collide and anyone can adopt one; a provider working with thousands of token projects described tying each to its website and social identity to disambiguate. Three design principles emerged: a wrapped or bridged

token is a different asset from its underlying and should carry the underlying's identifier plus its own; any bridging, wrapping or tokenisation that remains under a centralised service provider's control is a different asset again, because it adds that provider's risk; and tokenised real-world assets require a jurisdictional layer, because the claim they represent remains tied to the jurisdiction in which it was created. It was noted that ISO 24165 originates from ISO/TC 68/SC 8 (financial services) rather than ISO/TC 307 (blockchain and DLT), and that the liaison between both committees is the appropriate channel for proposing refinements. Participants also raised the business model of the registry, including the fee per identifier and the dependence on a single provider, and the possibility of a decentralised European registry. A proposal to address digital asset taxation through a 28th regime was judged politically unfeasible by other participants. A regulator present confirmed that identifiers are equally needed to reconcile transactions and detect market abuse under MiCAR, where the DTI is one option among several.

The third question was education. Participants reported that tax authorities lack the expertise to check or audit crypto-asset transactions, that the same gap exists at financial intelligence units, ombudsmen and police, and that in countries without a central tax authority the DAC8 reports will land at local offices with no experience of the asset class. One participant's filings had been on hold for almost two years because the authority could not read the broker reports. The proposed response was outreach through the tax advisers and accountants already connected to the industry associations, beginning with a first proposal developed in an association's tax working group and then shared with national associations across Europe.

Calls to Action regarding DAC8

The key calls to action from the discussion are:

- **Adopt one asset identifier across all reporting parties:** the Digital Token Identifier under ISO 24165 should be used consistently by CASPs, taxpayers and tax tooling, with a classification methodology that starts from the base asset, adds a jurisdictional layer for tokenised real-world assets, and adds the identifier of any service provider controlling a wrapped, bridged or tokenised version.
- **Define standard technical event scenarios:** the industry should attempt to specify which technical events (wrapping, bridging, forms of staking) entail an economic change and which do not, so that national tax concepts can be applied on top of a shared technical classification.
- **Narrow DAC8 reporting to its purpose:** reporting should be reassessed against the objective of detecting evasion and against proportionality; data that cannot be used to calculate tax or to identify non-filers should not be collected.
- **Educate the authorities through the advisers:** the associations should develop a first explanatory proposal through their tax working groups, covering identifiers,

event classification and what a taxable event is, and distribute it to tax advisers and national associations across Europe, with tax authorities invited to the next DARTE session on the topic.

- **Engage the standards bodies on identifier governance:** refinements to ISO 24165 should be proposed through the liaison between ISO/TC 68 and ISO/TC 307, and registry alternatives to a single provider should be examined.
- **Schedule the deferred proposals:** the second and third proposals should be taken up at a dedicated follow-up session.

3. CASP and PSP partnership models under MiCAR and PSD2/PSD3

The third topic, presented by Marina Villalonga, partner at Asensi Abogados, was a session on the overlap between MiCAR and the payment services framework, following discussions in São Paulo and Paris. The context was recalled briefly: CASPs that wish to operate with e-money tokens need, depending on the service, an authorisation under PSD2 in addition to their MiCAR licence; the draft of PSD3 resolved several interpretative questions about which services fall within payments and which remain under MiCAR; but the interim period until PSD3 applies is of unknown length. The question for this session was practical: how does a CASP that needs a payment authorisation structure a partnership with a payment service provider in a way that satisfies the EBA, ESMA and the supervisors involved.

The presentation, drawing on client work, set out five partnership structures. The agent model is the most common because the EBA's opinion refers to it expressly, but the opinion refers to it among others, so the market is not confined to it. The alternatives are an outsourcing model, a distribution agreement, a white-label model and hybrid or intra-group structures. Each allocates risk and obligations differently, so the choice determines the position of both CASP and PSP. Even within the agent model, open questions remain: whether the PSP needs a MiCAR licence, how strong customer authentication is allocated, how the overlapping safeguarding obligations interact, and the triangular passport problem, in which the PSP is registered in one Member State, the CASP in a second and the end user resides in a third, with no coordination between the three. In Spain the difficulty is compounded by two supervisors, the Banco de España for the PSP and the CNMV for the CASP, neither of which has issued guidance on these arrangements. The underlying question is who the client belongs to.

The discussion mapped supervisory practice across jurisdictions. Where the payment and crypto supervisors are separate authorities, dual licensing of a single entity has been permitted only in limited cases and is regarded as creating supervisory complexity; a memorandum of understanding on information exchange between the two authorities has been put in place, and the central bank in question is described as conservative in granting e-money and payment institution licences, with the consequence that obtaining one takes far longer than a

CASP licence. Where a single authority supervises both regimes, a different approach has emerged: the authority asks at the outset whether a CASP applicant will be affected by the overlap and processes a limited payment institution application alongside the CASP application in a streamlined workstream handled by the same authorisation team. In a third jurisdiction the authority expressed a preference for one entity holding both licences over two entities bound by a partnership, noted that the dual requirement had caused smaller applicants to withdraw, and called for clarification at legislative level. Market practice in Spain runs the other way: partnership is the first structure clients consider, and dual licensing comes second.

Several constraints on the partnership route were identified. A supervisor receiving a partnership structure has required a comprehensive legal opinion addressing liability, risk and custody, which the authority may or may not accept; this adds significant cost, deters first movers in a grey area, and was characterised by participants as regulation by enforcement, with authorities leaving the market to construct arrangements and judging them afterwards. The allocation of risk by contract is limited by mandatory rules: each party retains its own obligations before its own authority and cannot shift them to the other, so partnership is a misnomer for what is in substance the contracting of a service into one's own business. Client transparency follows from the structure chosen: whether the end client contracts with one party or two, whether the PSP is disclosed, and how a service failure reaches the client through the operational service levels. On capital, participants were surprised to learn that the own-funds requirements of MiCAR and PSD2 are not offset in a single entity but held as separate amounts, a position supervisors present confirmed on prudential grounds. On passporting, a dual-licensed entity notifies each supervisor separately for its respective licence. Regulatory arbitrage between national authorities was noted on both the MiCAR and the payments side, with centralisation of certain licences at ESMA raised as a possibility some Member States would welcome and others oppose.

The session converged on a pragmatic reading. A partnership is a time-to-market solution: a CASP launches under an agent or white-label arrangement, learns the business, and internalises it by obtaining its own licence once the service has proved itself, a pattern familiar from fintech, where the learning period ran to around three years. Participants did not want supervisory guidelines on how to structure partnerships, which they regarded as prescribing commercial choices; what they wanted was a use-case portfolio showing how others had structured arrangements, how risk and client relationships were allocated, and how supervisors had received them, usable both across jurisdictions and to educate regulators. Where regulatory clarity is needed, it lies upstream: when exactly a CASP's activity involving e-money tokens, such as trading against a stablecoin or settling it to a third-party custodian, triggers a payment service. With that fixed, the choice between structures becomes a commercial analysis of cost, reporting burden and client ownership. Participants also noted that submitting questions to the EBA Q&A process without prior industry alignment has previously been held back by market

participants, and that alignment within the industry should precede any approach to the authorities.

Calls to Action regarding CASP and PSP partnership models

The key calls to action from the discussion are:

- **Build a use-case portfolio of partnership structures:** the industry should document real agent, outsourcing, distribution, white-label and intra-group arrangements, including risk allocation, client contracting, service levels and the supervisory response, and share it across jurisdictions and with regulators as the alternative to prescriptive guidelines.
- **Obtain clarity on the trigger, not on the structure:** the EBA and ESMA should specify when activities involving e-money tokens, including trading against a stablecoin and settlement to a third-party custodian, constitute a payment service requiring authorisation, so that the choice of structure becomes a commercial decision.
- **Streamline joint applications where the overlap is foreseeable:** national authorities should ask CASP applicants at the outset whether they will be affected by the overlap and process a limited payment institution application alongside the CASP application, following the single-authority model already in use; where supervisors are separate, a memorandum of understanding should cover the exchange of information.
- **Clarify the capital treatment of dual-licensed entities:** the legislator should determine whether the own-funds requirements under MiCAR and the payments framework may be counted jointly within a single entity or must be held separately, as supervisors currently require.
- **Treat partnership as an interim structure:** CASPs should plan the partnership as a learning period with a defined path to their own licence, and should align within the industry before submitting Q&A questions to the authorities.

Closing remarks

The remarks by Jason Jiang from CertiK, contrasted the DARTE approach, in which the industry discusses a problem among itself before presenting to regulators and lawmakers, with the direct engagement with regulators that the firm is accustomed to in other jurisdictions: the latter produces direct answers, but leaves each participant isolated from the concerns of others. The topics of the day, dual licensing and the naming of assets among them, were described as touching some of the most fundamental issues the industry faces.

We thank all participants of the Madrid 3.0 DARTE event for contributing to the discussion:

Albi Rodriguez Jaramillo (Garrigues), Alessandro Fuser (Crypto Finance Group / Deutsche Börse), Almudena de la Mata (Blockchain Intelligence), Ana Alvarez, Andrea Disaró (DeFi), Belen Perulles (BBVA), Carlos António (Banco de Portugal), Carmen Arjona García (Asensi Abogados), Carol (MERGE), Daniela Corredor (Alastria), Eleonora Bellotto (Range), Elisa Martínez Simón (Inverco), Enrique Palacios Rojo (Bit2Me), Eu Cabrera (Alastria), Eugenio Reggianini, Fernando Carrillo Martínez (Deutsche Bank), George Theocharides, Gloria Hernández Aler (finReg360), Horacio Gómez Rey (N26), Irene Tagliamonte (Consob), Jason Jiang (CertiK), Jordan Wain (Chainalysis), Juan Cardona, Juan Ignacio Ibáñez (MiCA Crypto Alliance), Juan Jimenez Zaballos (Banco Santander), Justine Scerri Herrera (MK Fintech Partners), Lucia Suarez (Banco Santander), Luis Ayala (BitGo), Maria del Sagrario Navarro Lérida (UCLM), Maria Jose Ruiz de Olano Gallardo (Etherea Legal), Mariana de la Roche (BlackVogel), Marie Rinke (MÖHRLE HAPP LUTHER), Marina Villalonga (Asensi Abogados), Miguel Ángel Calero (Alastria), Neil Samtani, Nicky Gomez (XReg Consulting), Nina-Luisa Siedler (siedler legal), Nurtilek Taalaibekov (CertiK), Rebeca Brum dos Reis (BlackVogel), Robert de Groot, Santiago Martin Caravaca (Futura Legal), Sebastián Beltrán (Trace Global), Silvia Domíngez (Crypto Finance), Sol Cinosi (Association for Women in Cryptocurrency), Syed Choudhury (Range), Tamara O'Garra, Tommaso Astazi (Blockchain for Europe)