AKURATECO

2026

AKURATECO WHITEPAPER · EU REGULATORY BRIEFING

After MiCA: how payment orchestration helps crypto exchanges build *resilient fiat infrastructure*

A strategic whitepaper for Heads of Payments, COOs, and CFOs at EU crypto exchanges and crypto-asset service providers.

294

Authorised CASPs in the ESMA register

10M+

EU users facing migration

700+

Payment integrations via Akurateco



Andrew Riabchuk

Founder & CTO, Akurateco

CONTENTS

What's inside

01 **Executive Summary**
The compression of the EU crypto market, and the four payment gaps the survivors inherited.

02 **The End of the Wild West**
Banking by tolerance · the transition timeline · where authorizations landed · the Binance test.

03 **What MiCA Changed for Payments, Not Only Trading**
The CASP passport · the EMT problem · PSD2 triggers · SCA · the Tether precedent · PSD3 outlook · the fiat–crypto asymmetry.

04 **The Orchestration Gap**
The passport you cannot use · the migration surge · acquirer concentration · two clocks, one ledger · provable, not merely possible.

05 **Orchestration as the Operating Answer**
Local coverage · absorbing migration · routing & cascading · one data surface · evidenceable operations · the closed-loop model.

06 **Practical Readiness Checklist**
Fourteen questions a newly authorized CASP should be able to answer with evidence.

07 **Conclusion**
The next narrowing is operational — separating firms that hold a passport from firms that can use it.

— **About Akurateco · Sources**
Company profile and the references behind this edition.

01 SECTION 01 Executive Summary

MiCA has compressed the European crypto market. The maximum transitional period for legacy providers ended on 1 July 2026, and firms that had not secured authorization were expected to stop onboarding, marketing, and providing ordinary crypto-asset services to EU clients while completing an orderly wind-down.

244	294	1,738	10M+
Authorised firms at the 1 Jul 2026 deadline	CASPs in ESMA's register by 16 Jul 2026	Firms required to stop under the old rules	EU users facing a forced migration

The scale of that compression depends on the dataset and the date used. At the deadline, one widely cited market count placed the number of authorized firms at 244, compared with 1,738 firms required to stop operating under the old arrangements. Another industry dataset counted more than 3,300 previously registered entities across Europe. ESMA's own register continued to grow after the deadline, listing 294 authorized crypto-asset service providers by 16 July 2026. These figures should not be collapsed into a single percentage — they use different denominators and cut-off dates — but they point in the same direction: Europe moved from a fragmented registration market with thousands of entities to a much smaller authorization market with fewer than 300 firms in the official register by mid-July.

Industry participants estimated that more than 10 million European users could be forced to look for a new platform as unlicensed providers restricted or closed services. That figure is an industry estimate rather than an official EU statistic, but it captures the operational reality: the deadline created a concentrated migration event, not a gradual change in consumer behavior.

Binance became the most visible example. The exchange withdrew its Greek MiCA application shortly before the deadline and restricted services for affected EU users from 1 July. The sequence matters because it shows that scale, global brand recognition, and large compliance budgets did not remove the need to satisfy a national competent authority within the regulatory timetable. Binance is the example, not the argument. The argument is that the firms which cleared authorization inherited a market opportunity without automatically inheriting payment infrastructure designed for that market.

> *The survivors inherited a licensed market. They did not inherit the infrastructure built for it.*

Four gaps now define the next stage of competition.

01

A passport without local rails

A MiCA passport grants legal permission to serve multiple markets, but not local payment methods, local acquiring, or localized deposit flows.

02

A migration-driven volume spike

Displaced users create sudden onboarding and first-deposit volume that can expose capacity limits, velocity controls, and weak failover.

03

Acquirer concentration

Single-provider dependency remains a business-continuity risk in a vertical where risk committees can still reduce exposure.

04

Reporting that must be provable

Evidence must now hold up across MiCA, AML, and — where e-money token activity qualifies as a payment service — PSD2.

This paper argues that payment orchestration is the operating layer that helps close those gaps. It does not replace authorization, legal analysis, safeguarding, AML controls, or regulatory accountability. It makes a multi-provider fiat stack easier to localize, route, reconcile, monitor, and evidence. For a licensed crypto exchange, that distinction is critical: compliance establishes the right to operate; resilient payment infrastructure determines whether the right can be used at scale.

How ready is your fiat stack for a licensed EU market?
Akurateco maps localized deposits, multi-acquirer failover, and audit-ready evidence against the gaps MiCA exposed.

Get a readiness review →

02 SECTION 02 The End of the Wild West

2.1 What "Wild West" Meant Operationally

Before MiCA, crypto businesses operated through national VASP, DASP, or equivalent registration regimes that differed materially from one member state to another. A registration in one jurisdiction did not create a general right to provide services across the Union. Firms accumulated registrations, relied on reverse-solicitation arguments, served EU users from entities outside the bloc, or accepted significant uncertainty about where and how they could operate.

For payment teams, the most important consequence was not abstract regulatory fragmentation. It was **banking by tolerance**. A crypto exchange could hold a signed acquiring agreement and still understand that the relationship existed only while the acquirer's risk committee remained comfortable with the vertical, the jurisdictions, the transaction profile, the exchange's controls, and the wider political environment. The commercial contract mattered. The risk appetite behind it mattered more.

The familiar scenario was not necessarily a formal breach. It was a quarterly risk review, a revised underwriting policy, a sudden request for more information, tighter reserves, lower limits, or a notice that crypto exposure would be reduced. Sometimes the exchange received several weeks to migrate; sometimes a key route degraded before a replacement was ready. Any experienced Head of Payments in the sector recognizes the pattern: approval rates fall, deposits queue, customer-support volume rises, and engineering is asked to move traffic before the alternative integration has been fully tested.

The architecture that emerged was defensive and manual. Exchanges signed multiple PSP and acquirer contracts but integrated them one by one. Failover was partly automated, partly procedural, and often dependent on engineering. Reconciliation was performed separately for each provider. Decline codes were normalized in spreadsheets. Local payment methods were added market by market. Reporting data sat across dashboards, exports, internal databases, and finance tools. The stack was not irrational — it was a rational response to fragile provider relationships. The problem is that this legacy design is poorly suited to a harmonized authorization regime, rapid cross-border expansion, and regulator-ready evidence.

MiCA therefore changes the value of the old workaround. What once looked like prudent redundancy can become a fragmented control environment. A business may have five providers and still lack automatic failover, centralized routing governance, a unified audit trail, and a consistent view of settlement.

> *Redundancy is only useful when it can be operated as one system.*

2.2 The Transition Timeline

The dates matter because two separate transitions were running in parallel — and payment teams were accountable for both.

REGULATORY TIMELINE

Date	What changed	Payments relevance
29 Jun 2023	MiCA entered into force after publication in the Official Journal.	The legal framework existed before its main provisions became applicable.
30 Jun 2024	Titles III and IV, for asset-referenced tokens and e-money tokens, began to apply.	Stablecoin issuance and EMT treatment moved into the MiCA framework.
30 Dec 2024	The remaining MiCA provisions, including the CASP regime, became applicable.	CASP authorization and passporting became the core route to EU market access.
10 Jun 2025	The EBA published its No-Action letter on the PSD2–MiCA overlap for EMT-related services.	The EBA defined which EMT activities should be treated as payment services in the interim period.
2 Mar 2026	The EBA's recommended transition ended for in-scope EMT services.	CASPs providing qualifying EMT services needed PSP authorization or a partnership with an authorized PSP.
1 Jul 2026	The maximum MiCA transitional period ended.	Unauthorized providers were expected to stop normal EU operations and wind down in an orderly manner.

The public conversation focused on the end of the CASP grandfathering period, but payment teams also had to clear the earlier EMT deadline. A firm could be progressing toward a MiCA authorization while already needing to resolve a PSD2 question for specific services involving e-money tokens.

2.3 Where the Authorizations Actually Landed

The market snapshot changed quickly around the deadline. Public reporting counted 244 authorized firms as the transitional period ended, while ESMA's weekly register had increased to 294 by 16 July. This is why static claims such as "only 17% survived" should be used cautiously: the numerator changes weekly, and the denominator depends on whether the comparison includes active firms, legacy national registrations, duplicate legal entities, dormant registrations, or the broader EEA.

The more defensible conclusion is structural rather than arithmetic — **authorization concentrated market access**. The pre-MiCA system rewarded the ability to assemble national registrations. The post-transition system rewards the ability to satisfy a home regulator, passport services correctly, maintain governance and prudential controls, and operate a service-specific authorization scope. A firm listed as a CASP is not automatically authorized for every crypto-asset service: custody, transfer, exchange, execution, and operation of a trading platform are separate permissions in the ESMA data.

Jurisdiction shopping did not disappear; it changed form. MiCA created a common rulebook and passport, but the application is still assessed by a national competent authority. Applicants continue to compare regulatory capacity, supervisory approach, processing timelines, language, local substance expectations, and the availability of banking and talent. The difference is that the chosen jurisdiction now determines the home authorization underpinning cross-border activity, rather than simply adding another registration to a patchwork.

Licensed competitors are using the moment commercially. Exchanges already operating under MiCA have launched migration pages, reassurance campaigns, and targeted offers to users of firms that missed the deadline. This creates a narrow window in which payment performance directly affects customer acquisition. The winning exchange is not only the one with the license; it is the one that can complete KYC, accept a first deposit through a familiar method, manage authentication, and make the first funding experience feel reliable.

MARKET SNAPSHOT — USE DATES AND DEFINITIONS EXPLICITLY

Snapshot	Figure	How to use it
At the 1 Jul 2026 deadline	244 authorized firms in widely cited reporting	A deadline snapshot, not the permanent total.
ESMA update, 16 Jul 2026	294 authorized CASPs	The latest official-register count for this edition.
Legacy market size	~2,000 active firms to 3,300+ registered entities, depending on the dataset	Do not derive a single "survival rate" without naming the dataset.
Potential user migration	10M+ users (industry estimate reported by CoinDesk)	Label clearly as an estimate, not an official EU number.

2.4 Binance: A Visible Test of the Authorization Bar

Binance applied for a MiCA authorization in Greece and withdrew the application shortly before the end of the transition period. Reporting around the application included disagreement over whether the file was likely to be rejected, whether the review had effectively been completed, and how much weight ESMA's concerns carried. The legal point is straightforward: ESMA coordinates and promotes supervisory convergence, but a national competent authority grants or refuses a CASP authorization.

After the withdrawal, Binance communicated restrictions to affected EU clients. Reporting identified France, Italy, Poland, and Spain among the markets where customers were told that ordinary services would no longer continue from 1 July, while withdrawals and actions necessary for an orderly exit remained available. Binance said it was not abandoning Europe and intended to pursue authorization in another member state.

Binance's European leadership framed the outcome as a question about whether the success of MiCA should be measured by the existence of regulation or by bringing major market participants inside the regulated perimeter. The company also emphasized its global compliance investment and staffing.

The relevant operational conclusion is narrower. If the world's largest exchange, with substantial compliance resources, could not complete the process within the available timetable, authorization cannot be treated as an administrative formality. For the firms that did secure it, the next test begins immediately: turning regulatory permission into reliable market access.

SECTION 03

03 What MiCA Changed for Payments, Not Only for Trading

Most MiCA explainers focus on authorization, investor protection, stablecoin classifications, governance, and market abuse. Far fewer explain the payments asymmetry created by e-money tokens: a transfer of a euro-referenced token on behalf of a client can sit inside both the crypto-asset and payment-services frameworks, while an economically similar fiat payment is governed through the payments framework alone. The EBA has described the resulting dual-authorization burden as undesirable and asked legislators to resolve it.

3.1 CASP Authorization and the Passport

A CASP authorization can cover services including custody and administration of crypto-assets, operation of a trading platform, exchange of crypto-assets for funds or for other crypto-assets, execution and transmission of orders, advice, portfolio management, and transfer services. The exact service scope matters: a firm authorized for custody and transfer is not automatically authorized to operate a trading platform.

Once authorized, a CASP can provide the authorized services cross-border through MiCA's passporting framework, subject to the notification process and other requirements. For management teams, the strategic promise is significant — one home-state authorization can support access across the EU rather than a stack of separate national crypto registrations.

The passport is nevertheless a legal permission, not an operational capability. It does not create a local acquiring relationship, a BLIK connection in Poland, iDEAL access in the Netherlands, Wero readiness in Germany or France, Bizum acceptance in Spain, or a localized deposit UX. It tells the exchange *where* it may operate. It does not build the payment rails needed to compete there.

3.2 The EMT Problem

MiCA distinguishes three broad categories. An **e-money token (EMT)** seeks to maintain a stable value by referencing one official currency. An **asset-referenced token (ART)** references another value, right, or combination of values — including one or more official currencies — but is not an EMT. **Other crypto-assets** include categories such as utility tokens.

EMTs have a dual legal character. MiCA treats them as crypto-assets but also connects them to the EU electronic-money framework. Article 48 requires an EMT issuer to be authorized as a credit institution or electronic money institution, and Article 49 establishes issuance and redemption at par. MiCA also prohibits interest on EMTs. This is more precise than saying that every EMT is simply "regulated under PSD2": the issuer regime sits in MiCA and the electronic-money framework, while specific CASP activities involving EMTs can also qualify as payment services.

The overlap became operationally important because a CASP may do more than list or exchange a token. It may custody EMTs for a client, operate a custodial wallet that can send and receive EMTs, or transfer EMTs on the client's behalf. The EBA concluded that some of these activities should be treated as payment services during the interim period, creating a potential requirement for a second authorization under PSD2 or a partnership with an authorized PSP.

On 10 June 2025, the EBA published a No-Action letter developed in coordination with ESMA. The letter did not eliminate the overlap; it reduced and sequenced enforcement while the EU institutions continued work on PSD3 and the Payment Services Regulation. The EBA recommended streamlined authorization procedures that reuse information already submitted in a MiCA application, and gave firms until 1 March 2026 to obtain the necessary PSP authorization or partnership. From 2 March, national authorities were advised to prevent unlicensed entities from continuing qualifying EMT payment services.

> *The practical test is not "is this crypto?" It is "are we holding or moving an EMT on behalf of a client?"*

3.3 What Triggers PSD2 — and What Does Not

The EBA's interim approach is practical enough to convert into an operating decision table. It should still be applied with legal advice, because the facts of a product, wallet design, client relationship, and transaction flow matter.

EMT ACTIVITY AND THE EBA'S INTERIM PSD2 TREATMENT

Activity	Interim PSD2 treatment	Operational implication
Transfer of crypto-assets where the transfer entails EMTs, carried out on behalf of clients	**Treat as a payment service**	PSP authorization or a partnership with an authorized PSP may be required.
Custody and administration of EMTs where the custodial wallet can send and receive EMTs to and from third parties	**Treat as a payment service;** the wallet is treated as a payment account	Wallet access, authentication, fraud reporting, and own-funds implications must be assessed.
Exchange of crypto-assets for funds, as defined in MiCA	**Do not treat** as a payment service merely because EMTs are involved	A MiCA exchange service does not automatically create a PSD2 licensing requirement.
Exchange of crypto-assets for other crypto-assets, as defined in MiCA	**Do not treat** as a payment service	Own-account exchange remains outside the EBA's selected PSD2 scope.
Intermediation of a client's purchase of crypto-assets using EMTs	**Do not treat** as a payment service under the interim approach	The EBA sought to avoid extending PSD2 to a broad range of purchase intermediation.

For a legacy VASP, the distinction is substantial. A national VASP registration generally addressed crypto-related activities under the relevant national AML or registration framework. It did not by itself authorize the firm to issue electronic money, hold customer fiat as a payment institution, or provide regulated payment services. MiCA authorization improves the crypto-services perimeter; it does not retrospectively convert a VASP registration into a payments license.

3.4 SCA on Custodial Wallet Access and EMT Transfers

The EBA recommended that national authorities deprioritize enforcement of selected PSD2 requirements that are difficult to map cleanly onto distributed-ledger services — including parts of the safeguarding, information-disclosure, unique-identifier, and open-banking rules. It did not recommend deprioritizing the core security and supervisory-data requirements indefinitely.

Authorities were advised to insist on strong customer authentication (SCA) for access to custodial wallets treated as payment accounts and for the initiation of EMT transfers. The EBA also identified payment-fraud reporting and the cumulative calculation of own-funds requirements as priorities. Supervision and enforcement of SCA and selected fraud-reporting requirements were temporarily deprioritized until 2 March 2026 — that period has ended.

For a Head of Payments, SCA is not a sentence in a legal memo. It is an event inside a money-movement journey. It affects authentication success, abandonment, customer support, device recognition, recovery flows, and fraud strategy. An exchange that previously treated wallet login as a standard account-access event may now need to distinguish access to a custodial payment account, transaction initiation, high-risk actions, and the evidence retained for each authentication decision.

This does not mean a payment orchestrator can declare the exchange compliant. The useful infrastructure role is narrower: normalize authentication results across providers, route transactions according to supported authentication paths, centralize outcome data, and measure where friction or technical failures occur. Legal responsibility remains with the regulated firm and its authorized partners.

3.5 The Tether Precedent: Asset Choice Became Infrastructure Risk

USDT became the clearest example of how issuer-level regulatory choices can change an exchange's product and payment architecture. Tether did not establish a MiCA-authorized EU issuance structure for USDT, and major exchanges restricted or removed trading pairs involving non-MiCA-compliant stablecoins for EEA clients. Binance announced the removal of affected spot pairs from 31 March 2025, and Kraken implemented a staged change to its EEA stablecoin offering.

The reason should not be reduced to a single reserve-percentage slogan. MiCA's EMT regime includes issuer authorization, issuance and redemption obligations, investment rules, governance, and additional requirements for significant tokens. The core operational fact is simpler: an exchange may depend on an asset whose issuer chooses not to enter or remain in the EU regulatory perimeter. When that happens, the exchange must change listings, pairs, treasury processes, liquidity relationships, customer communication, and potentially the rails used for deposits and withdrawals.

The general lesson is that asset support is no longer only a product or liquidity decision — it is a regulatory dependency. Payment and treasury architecture should therefore be designed for substitution: compliant stablecoin options, fiat alternatives, configurable settlement logic, and the ability to change routes without rebuilding the entire on-ramp.

3.6 Forward Look: PSD3 and the Payment Services Regulation

The EBA described its 2025 approach as an interim solution pending PSD3 and the Payment Services Regulation. By July 2026, the legislative package had reached an advanced stage: Parliament and Council reached a provisional political agreement on 27 November 2025, and the compromise texts advanced through the EU's formal approval steps during the first half of 2026. It had not yet completed every formal step required for final adoption and publication.

The negotiated texts include mechanisms intended to reduce unnecessary duplication and to streamline applications by MiCA-authorized CASPs seeking authorization to provide payment services. The exact long-term treatment of EMT-related services should be assessed against the final published legislation once adopted, and its application and transposition dates are known.

The strategic direction is already visible. EMT activity that functions like payments is converging with the payments rulebook rather than being exempted from it. A CASP should therefore build authentication, fraud data, customer protection, operational resilience, and reporting capabilities that can survive a change in legal architecture. Building only for the temporary interpretation is a short-lived strategy.

3.7 The Fiat–Crypto Asymmetry

The surprising asymmetry can now be stated precisely. A euro-denominated fiat transfer provided by an authorized payment institution sits within the payments regime. A transfer of a euro-referenced EMT on behalf of a client can require a MiCA-authorized CASP perimeter and, under the EBA's interim approach, a PSD2-authorized payment-services perimeter or partnership. The same user intent — moving euro-linked value — can therefore create two authorization layers when the value is represented as an EMT.

The EBA considers that duplication disproportionate and has asked EU legislators to prevent unnecessary dual authorization. Until the legislative solution is final and applicable, the asymmetry remains a real operating constraint. For management teams, the right response is not to assume that "crypto regulation" and "payments regulation" can be handled by separate teams. Product design, legal classification, payments operations, fraud, and treasury must work from the same transaction map.

04 SECTION 04 The Orchestration Gap

4.1 The Passport You Cannot Use

Imagine an exchange authorized in one member state and ready to passport its services. The legal team can name the markets. The commercial team can launch campaigns. The payment team then discovers that the deposit experience is still card-first, routed through one cross-border acquirer, and localized only by language and currency.

That is not a usable passport. Dutch users expect iDEAL and are gradually being introduced to Wero; Polish users fund online transactions through BLIK and local bank-payment experiences; Germany combines cards with PayPal, SEPA, invoice-oriented habits, and a growing Wero rollout after the closure of giropay; France has strong domestic card-scheme relevance and an expanding Wero ecosystem; Spain has Bizum; Italy has BANCOMAT and account-based options; the Nordics are shaped by Vipps, MobilePay, and Swish. The mix keeps evolving as European wallet schemes become interoperable.

The lesson is not that every exchange must integrate every local method on day one. It is that market access must be prioritized by actual funding behavior, local banking coverage, user economics, and regulatory constraints. A passport creates the right to enter; a payment-coverage plan determines whether customers can fund accounts in a way they trust.

EXAMPLES OF MARKET-SPECIFIC FUNDING EXPECTATIONS

Market	Relevant methods and rails	Why a card-only flow is insufficient
Netherlands	iDEAL, cards, wallets, emerging Wero migration	Account-to-account payment behavior is deeply established.
Poland	BLIK, local bank transfers, cards and wallets	BLIK is a mass-market behavior — more than 21 million active users reported in Q1 2026.
Germany	PayPal, SEPA, cards, invoice-oriented methods, Wero	Giropay is no longer a valid 2026 assumption; the market is moving to new account-based options.
France	Cartes Bancaires ecosystem, cards, SEPA, Wero	Domestic scheme and bank-led wallet coverage affect acceptance and familiarity.
Spain	Cards, Bizum, bank transfers	Bizum is embedded in bank apps and used online and in person.
Italy	Cards, BANCOMAT, bank transfers and wallets	Domestic account and wallet ecosystems remain strategically relevant.
Nordics	Vipps, MobilePay, Swish, cards and account payments	Mobile-wallet expectations differ materially from a generic EU checkout.

4.2 The Migration Surge

A large provider's exit does not create a smooth, forecastable acquisition curve. It creates a cluster of onboarding, KYC, first-deposit, support, and withdrawal events. Campaigns from licensed exchanges can compress that activity further by encouraging users to move before a deadline or promotional window closes.

The first failure often appears outside the core ledger. A single acquirer reaches a velocity threshold. A 3DS path degrades. A provider's risk model reacts to an unfamiliar spike. A local payment method is unavailable in the market where the campaign performs best. The exchange sees "issuer declines" in one dashboard, "risk declines" in another, and a rise in abandoned KYC sessions that may actually be caused by deposit friction.

Capacity must therefore be understood as more than transactions per second. It includes provider headroom, acquiring limits, fraud-review capacity, authentication throughput, webhook handling, ledger posting, reconciliation processing, customer support, and the speed with which traffic can be redistributed. Rails designed for organic growth can fail during a competitor-driven demand shock even when the exchange's own infrastructure remains technically online.

4.3 Acquirer Concentration

MiCA authorization improves the credibility of the exchange, but it does not eliminate the acquiring bank's independent risk appetite. The acquirer still weighs financial-crime exposure, sanctions risk, chargebacks, card-scheme monitoring, transaction geography, user behavior, reserve requirements, and concentration in the crypto vertical.

Single-acquirer dependency therefore remains one of the most dangerous hidden risks in a licensed exchange. The relationship can be perfectly healthy on Monday and subject to reduced limits, new reserves, or an exit decision after a risk review. If most fiat deposits depend on that route, the exchange's legal right to operate does not prevent its front door from closing.

> *For a crypto exchange, multi-acquirer routing is not conversion optimization. It is business continuity.*

4.4 Two Clocks, One Ledger

Fiat and on-chain systems settle according to different clocks. Card acquiring follows authorization, clearing, settlement, reserves, refunds, and chargeback timelines. Bank payments follow scheme cut-offs, value dates, return windows, and reconciliation files. On-chain transfers follow block production, confirmations, network fees, chain reorganizations, and wallet controls.

The exchange must join these worlds at transaction level. A user's fiat deposit may be authorized before it is settled. A crypto withdrawal may occur before a card chargeback arrives. A bank transfer may be returned after a provisional credit. A stablecoin movement may be final on-chain while the corresponding fiat-side funding remains subject to reversal or reserve treatment.

Before MiCA, a reconciliation break could remain an internal operations issue for several days. In a regulated environment, unexplained breaks, inconsistent client balances, weak safeguarding records, or incomplete transaction lineage can become evidence of a control failure. The challenge is not merely matching totals; it is proving the relationship among the customer, the payment attempt, the provider response, the authentication event, the ledger entry, the fee, settlement, refund or return, and the resulting on-chain action.

4.5 Provable, Not Merely Possible

The operational shift fits in one line: before MiCA, a team needed to be *capable of answering* questions; after authorization, it needs to *demonstrate the answer on demand*. That distinction changes system design.

A supervisor, auditor, bank, or internal risk committee may ask which provider processed a transaction, which routing rule was applied, whether SCA was performed, what the provider returned, who changed the rule, how the customer balance was updated, when settlement occurred, and how the transaction was classified for fraud reporting. If the answer requires three dashboards, a data engineer, a finance spreadsheet, and an explanation from someone who remembers the incident, the firm does not have a robust evidence system.

MiCA record-keeping, AML transaction monitoring, operational-resilience expectations, and PSD2 fraud reporting for qualifying EMT activity do not all use the same definitions or cadence. The exchange therefore needs a payment data model that preserves raw provider evidence, normalizes fields for operations, and supports reproducible reporting. Data scattered across five PSP dashboards is not a reporting system.

> *You cannot reconcile two clocks from five dashboards.*

A passport is permission. Orchestration is access. Localize deposits, absorb migration surges, and route around acquirer risk — without rebuilding your on-ramp.

Request a demo →

05 SECTION 05 Orchestration as the Operating Answer

Payment orchestration should not be presented as a compliance shortcut. It does not grant a MiCA authorization, classify an EMT, replace a PSP license, perform the exchange's AML obligations, or decide whether a customer asset is safeguarded correctly. Its value is operational: it creates a control layer across providers, methods, routes, retries, data, and permissions so that the fiat side of the business can be run as one environment rather than a collection of integrations.

5.1 Turning the Passport into Local Payment Coverage

The first requirement is connectivity. Instead of building a separate integration for each acquirer, bank, wallet, or alternative payment method, the exchange connects to an orchestration layer that already supports a broad integration library and can add custom connectors. Akurateco describes its network as more than 700 integrations, with custom connectors available on request. For a licensed CASP, the decisive capability is not the headline number — it is the ability to prioritize and activate the right local rail without redesigning the checkout and core transaction system. The exchange keeps one internal payment contract while presenting different methods, currencies, provider routes, and user experiences by market.

This turns expansion into a configuration-and-integration program rather than a sequence of payment-stack rebuilds. Poland can launch with BLIK and local bank coverage; the Netherlands with iDEAL and a Wero migration plan; Spain with Bizum; Germany and France with the appropriate card, account, and wallet mix. The license opens the market on paper. Connector coverage opens it in practice.

5.2 Absorbing a Migration Event with Multi-Provider Capacity

A migration surge should be distributed before it becomes a provider incident. Orchestration lets the exchange define capacity-aware routes across multiple acquirers and methods, observe real-time performance, and reduce dependence on manual switching. The objective is not to spray identical traffic across every provider; it is to allocate traffic according to each provider's geography, limits, risk appetite, method support, cost, and observed performance.

A prebuilt orchestration layer shortens the work required to add and operate providers compared with a direct-integration program. Custom-connector timing still depends on the quality of the provider's technical documentation, certification requirements, access to its technical team, and testing.

Network tokenization can support migrated users who deposit repeatedly with cards. A network token can be updated when the underlying credential changes, reducing avoidable failures for stored-card use cases and limiting repeated entry of card details. It does not eliminate authentication or issuer decisioning, but it improves credential continuity and payment-data security.

Continuous payment-operations support can be valuable during a surge — particularly when teams are tuning routing, monitoring a new provider mix, or diagnosing authentication failures. This is operating support, not a substitute for the exchange's internal payment ownership.

5.3 Routing and Cascading as Business Continuity

Routing decides where a transaction should be attempted. Cascading decides what should happen when the selected route fails and a safe alternative exists. In a mature setup, neither decision is a static priority list. Rules can weigh market, currency, card type, transaction amount, customer segment, provider cost, provider availability, risk signals, authentication support, and performance history.

The continuity value appears when a provider's behavior changes. If one acquirer begins returning technical errors or unexpected declines, the orchestration layer can redirect eligible traffic to an alternative route without waiting for a new release. If the provider exits the vertical, the exchange can change routing centrally rather than rewriting multiple product integrations.

Cascading must be controlled. Reattempting a transaction through another acquirer can increase approvals, but uncontrolled retries create duplicate-authorization risk, scheme concerns, poor customer experience, and additional fraud exposure. The exchange needs idempotency, clear retry eligibility, normalized response codes, velocity controls, and rules that distinguish a soft decline, a hard decline, a technical failure, and an authentication requirement.

Akurateco states that routing and cascading can improve approval rates by **up to 30%**, including client examples. Results vary with the prior setup, provider mix, market, vertical, and decline profile, so the figure is an "up to" benchmark rather than a forecast for any specific exchange.

Risk controls belong inside the same discussion. Routing away from a declining acquirer is only sustainable if fraud controls remain calibrated by merchant, MID, market, and route. Akurateco describes configurable anti-fraud rules and external risk integrations, with controls applied at merchant, group, or MID level. The principle matters more than the module list: redundancy without risk calibration is how a firm loses the second acquirer after the first one exits.

5.4 One Fiat-Side Data Surface for Two Clocks

Orchestration can centralize provider responses, routing decisions, authentication outcomes, fees, refunds, settlement data, and operational events within one reporting environment.

The goal is not to replace the core ledger; it is to create a reliable join point. Every payment attempt should carry a stable internal identifier that survives provider retries. Provider transaction IDs, network references, authentication data, customer and account identifiers, settlement batches, and ledger postings can then be related without free-text notes or manual reconciliation.

> *One fiat-side data surface is the minimum condition for automation.*

5.5 Making Operations Evidenceable

Evidence begins with deployment and access design. A regulated exchange may need to answer questions about data location, infrastructure ownership, security boundaries, administrator access, operational resilience, and the responsibilities of third-party providers. Akurateco offers SaaS and on-premises deployment models, including deployment on infrastructure chosen by the client. That flexibility can support a regulator or risk-committee discussion about data residency and control, although it does not by itself satisfy any particular legal requirement.

Role-based access is equally important. Payment operations, fraud, finance, support, engineering, and compliance should not all hold the same permissions. Akurateco's admin-panel materials describe custom roles, granular permissions, transaction logs, and real-time data management. In a regulated environment these should be configured as a control model: separation of duties, approval of high-risk changes, traceability of routing-rule edits, and evidence of who accessed or changed sensitive data.

For PSD2 payment-fraud reporting on qualifying EMT services, the safe claim is that transaction and fraud data can be centralized and exported. Orchestration makes evidence easier to assemble; the regulated institution remains accountable for classification, completeness, and filing.

5.6 The Closed-Loop Model

FROM REGULATORY AND OPERATING PROBLEM TO ORCHESTRATION CAPABILITY

Problem established earlier	Required capability	What becomes possible
Passport without local rails	Connector coverage, custom integrations, localized methods and currencies	Enter each market with a funding experience aligned to local behavior.
Migration-driven volume spike	Multi-provider capacity, monitoring, tokenization, configurable traffic distribution	Absorb demand without discovering the ceiling of a single route during the event.
Acquirer concentration	Smart routing, controlled cascading, multi-acquirer failover, route-specific risk controls	Maintain the fiat on-ramp when a provider degrades or exits.
Two clocks and fragmented data	Normalized transaction data, stable IDs, data exports, settlement visibility	Join fiat events to the exchange ledger and on-chain records.
Compliance that must be provable	Granular permissions, logs, deployment control, centralized evidence	Reproduce who did what, which route was used, and how a transaction was handled.

Each capability earns its place by closing a problem established earlier — not by lengthening a feature list.

06 SECTION 06 Practical Readiness Checklist

For a newly authorized CASP, each question below should be answerable with evidence — not with an intention or a roadmap. A "no" identifies an operating risk that becomes more visible after authorization.

A · EMT SCOPE, AUTHORIZATION & AUTHENTICATION

- [ ] Do we custody or transfer any e-money token on behalf of clients, and has legal counsel documented whether each flow is a payment service under the EBA's interim approach?
- [ ] Where an EMT flow qualifies as a payment service, do we hold the required PSP authorization or a documented partnership with an authorized PSP?
- [ ] Is strong customer authentication implemented for the relevant custodial-wallet access and EMT-transfer flows, with measurable success, abandonment, and recovery data?

B · ASSETS & LOCAL MARKET COVERAGE

- [ ] Can we identify which supported stablecoins depend on an issuer authorized for the EU market, and can we replace an asset or settlement route without rebuilding the on-ramp?
- [ ] For every market in our MiCA passport plan, can users fund accounts through the locally relevant methods and acquiring routes — not only a generic cross-border card flow?

C · CAPACITY, ROUTING & CONTINUITY

- [ ] What percentage of fiat deposit volume depends on our largest acquirer, and what happens to onboarding and withdrawals if that route is unavailable for 24 hours?
- [ ] Can we route eligible traffic around a provider decline spike within minutes, without an engineering release or a manual ticket?
- [ ] Have we tested provider limits, authentication throughput, fraud operations, callbacks, ledger posting, and reconciliation at two, five, and ten times normal first-deposit volume?

D · DATA, RECONCILIATION & REPORTING

- [ ] Does every payment attempt have one internal identifier that survives retries and can be joined to provider records, the customer ledger, settlement data, and any related on-chain movement?
- [ ] Can finance produce a daily provider-level settlement and break report without manually combining dashboards and spreadsheets?
- [ ] Can compliance produce a transaction-level audit view — routing, authentication, provider response, user action, permissions, and rule changes — without engineering assistance?
- [ ] For qualifying EMT activity, do we capture the data required for PSD2 fraud reporting, and has the reporting owner validated definitions, cadence, and submission responsibility?

E · GOVERNANCE & CONTROL

- [ ] Are payment-operations roles separated so that no single user can create a route, change risk controls, and approve the same change without oversight?
- [ ] Can we demonstrate where payment data is hosted, who can access it, how changes are logged, and how continuity is maintained if a provider or deployment component fails?

07 SECTION 07 Conclusion

MiCA narrowed the European crypto market to firms that could clear a higher authorization bar. The official register continued to grow after the deadline, but the direction of travel is not in doubt: market access is becoming concentrated in authorized institutions with defined governance, capital, record-keeping, and conduct obligations.

The next narrowing will be operational. It will separate firms that possess a passport from firms that can use it. The winners will localize deposits market by market, absorb user migration without overloading one route, preserve the fiat on-ramp when an acquirer changes risk appetite, reconcile fiat and on-chain events through a consistent data model, and produce evidence without reconstructing the transaction from multiple dashboards.

Payment orchestration is not the license, and it is not the compliance function. It is the control layer that helps the payment stack catch up with the regulated business. It turns provider redundancy into managed continuity, local integrations into a repeatable expansion model, and transaction data into an audit-ready operating record.

> *“The license gets the exchange through the door. Orchestration helps keep the door open.*

See where orchestration fits your fiat stack

Talk to Akurateco about localizing deposits, adding multi-acquirer failover, and making payment operations evidenceable — without rebuilding your on-ramp.

Contact our team →

AKURATECO

About Akurateco

Akurateco is a payment orchestration platform founded in 2019 and headquartered in Portugal. Its offering connects businesses to more than 700 payment integrations and supports intelligent routing, cascading, tokenization, anti-fraud controls, centralized transaction monitoring, reporting, and flexible SaaS or on-premises deployment.

For crypto exchanges and CASPs, Akurateco's role is focused on the fiat payment layer. The platform does not orchestrate blockchain settlement, provide crypto custody, classify e-money tokens, or replace a regulated institution's legal and compliance responsibilities. It helps the exchange operate the banks, acquirers, payment methods, routes, and payment data that sit underneath the crypto product.

Learn more about Akurateco →

2019	Portugal	700+	PCI DSS L1
Founded	Headquarters	Integrations	Certified (SaaS)

REFERENCES

Sources

References for the figures, dates, and claims cited in this edition. Primary regulatory and legal texts are cited where available; platform data is from Akurateco materials. Sources accessed July 2026.

1 ESMA — Register of authorised crypto-asset service providers (interim MiCA register) and the statement on the end of the MiCA transitional period, 1 July 2026. esma.europa.eu

2 Legacy market size — ~3,000 pre-MiCA VASPs (Poland alone 1,400+) against ~230 authorised at the deadline. CoinDesk, 29 Jun 2026

3 Industry estimate of 10M+ EU users facing migration — Alex Fazel, SwissBorg. CoinDesk, 29 Jun 2026

4 EBA — No-Action letter on the PSD2–MiCA interplay for CASPs transacting EMTs (Opinion EBA/Op/2025/08, 10 Jun 2025) and its supervisory-priorities guidance as the transition ended, 2 Mar 2026. eba.europa.eu

5 MiCA — Regulation (EU) 2023/1114: EMT issuer authorisation and redemption at par (Articles 48–49), and the application-date timeline (Titles III–IV, 30 Jun 2024; CASP regime, 30 Dec 2024). eur-lex.europa.eu

6 Binance — withdrawal of the Greek MiCA application and EU service restrictions (France, Italy, Poland, Spain). CoinDesk · Euronews

7 Removal of non-MiCA stablecoin pairs for EEA clients (from 31 Mar 2025) — Binance (nine stablecoins incl. USDT) and Kraken's staged delisting. CryptoSlate · Crypto Briefing

8 PSD3 & Payment Services Regulation — Parliament–Council provisional political agreement, 27 Nov 2025; compromise texts approved by COREPER, Apr 2026. European Parliament

9 Domestic payment schemes referenced — iDEAL, BLIK, Bizum, Wero / EPI, Vipps MobilePay, Swish, BANCOMAT.

10 BLIK — 21.1 million active users at the end of Q1 2026 (Polski Standard Płatności). blik.com

11 Akurateco — platform materials: 700+ integrations, smart routing & cascading (up to 30% approval uplift), network tokenization, configurable anti-fraud, SaaS / on-premises deployment, PCI DSS Level 1, and admin-panel roles & permissions. akurateco.com