



GOVERNING THE DIGITAL EURO ECOSYSTEM

The role of Article 33 in standard-setting,
access and innovation

Judith Arnal and Apostolos Thomadakis

SUMMARY

As the digital euro project progresses from design stage to the implementation phase, the focus is shifting from fundamental principles to governance issues. Article 33 of the Digital Euro Regulation, currently under development, can be understood not just as a technical access rule but as a governance pivot between coordination at the scheme level and implementation by the markets.

A layered governance approach seems most appropriate. Coordinating interoperability requirements, security standards, certification processes and operational resilience makes sense at the scheme level, where consistent rules and standards are needed across the single market. However, wallet designs, customer interfaces, value added services and other implementations must be open to competition and innovation.

Accessing mobile-device functionality is the most sensitive issue. The final Regulation should establish a stand-alone Article 33 access regime, coordinated with the Digital Markets Act, that ensures effective and non-discriminatory access based on outcome criteria; it should also include measures that provide necessary and proportionate protection of system integrity.

The experience with the Single European Payments Area and Eurosystem TARGET services shows that the governance of an open, contestable and scalable digital euro ecosystem is best achieved through coordinated efforts, structured stakeholder participation and a predictable change management process.



Judith Arnal is an Associate Senior Research Fellow in the Financial Markets and Institutions (FMI) unit at CEPS. Apostolos Thomadakis is Head of the FMI unit at CEPS.

CEPS In-depth Analysis papers offer a deeper and more comprehensive overview of a wide range of key policy questions facing Europe. Unless otherwise indicated, the views expressed are attributable only to the authors in a personal capacity and not to any institution with which they are associated.

CONTENTS

1. INTRODUCTION	2
2. ARTICLE 33 – THE GOVERNANCE HINGE OF THE DIGITAL EURO ECOSYSTEM	4
2.1. THE EVOLVING ROLE OF ARTICLE 33 IN THE LEGISLATIVE NEGOTIATIONS	6
3. WHAT NEEDS TO BE STANDARDISED AND WHAT CAN STAY OPEN?	10
3.1. COMPONENTS OF THE DIGITAL EURO ECOSYSTEM THAT REQUIRE COMMON EUROPEAN STANDARDS	10
3.2. AREAS FOR WHICH MARKET-DRIVEN IMPLEMENTATION IS APPROPRIATE	11
3.3. PRINCIPLE OF TECHNOLOGICAL NEUTRALITY	12
4. ACCESS, CONTESTABILITY AND IMPLEMENTATION SCALABILITY	14
4.1. ARTICLE 33 AND THE DMA: COORDINATION, NOT INCORPORATION	15
4.2. OUTCOME-BASED ACCESS AND TECHNOLOGICAL NEUTRALITY	17
4.3. ACCESS GOVERNANCE, ENFORCEMENT AND SCALABILITY	18
5. LESSONS LEARNED FROM CURRENT EUROPEAN SYSTEMS	20
5.1. SEPA: STANDARDISED APPROACH, DECENTRALISED IMPLEMENTATION	20
5.2. TARGET SERVICES: OPERATIONAL GOVERNANCE AND RESILIENCE	20
5.3. IMPLICATIONS FOR THE GOVERNANCE OF THE DIGITAL EURO	22
6. OPERATIONAL GOVERNANCE FOR THE DIGITAL EURO	23
7. CONCLUSIONS	26

TABLES AND BOX

TABLE 1. A LAYERED GOVERNANCE FRAMEWORK FOR THE DIGITAL EURO ECOSYSTEM	6
TABLE 2. TREATMENT OF ARTICLE 33 ACROSS THE MAIN LEGISLATIVE TEXTS	7
TABLE 3. INDICATIVE ALLOCATION OF STANDARDISATION RESPONSIBILITIES WITHIN THE DIGITAL EURO ECOSYSTEM	12
TABLE 4. GOVERNANCE FEATURES OF EXISTING EUROPEAN PAYMENT INFRASTRUCTURES AND THEIR RELEVANCE FOR THE DIGITAL EURO	21
TABLE 5. PILLARS OF AN OPERATIONAL GOVERNANCE FRAMEWORK FOR THE DIGITAL EURO	23
BOX 1. ARTICLE 33 – FAIR, REASONABLE AND NON-DISCRIMINATORY ACCESS TO MOBILE DEVICES	4

1. INTRODUCTION

The debate over the digital euro is entering a new phase. In previous discussions, much attention was paid to whether Europe needs a central bank digital currency (CBDC), and the objectives that such a tool could pursue. The issues of monetary sovereignty, strategic autonomy, resilience, financial inclusion and the role of public money in a digitised economy were discussed in depth. However, the focus is increasingly shifting from these topics to an important but often overlooked aspect of the discussion – the governance of the digital euro ecosystem.

This shift reflects the increasing maturity of the digital euro project. With the development of legal and technical frameworks and the preparation for the project implementation, the success of the initiative cannot be ensured without establishing an adequate and flexible governance regime. The question today is not whether the digital euro could exist, but how the ecosystem surrounding this new tool should be organised. In other words, beyond the question of its existence, there is the challenge of creating a viable ecosystem for the new tool.

The legislative context is the single-currency package proposed by the Commission in June 2023. It comprises: i) the proposed [Regulation on the establishment of the digital euro](#) (i.e. the proposed Regulation), which also gives the digital euro legal-tender status; ii) a separate proposed [Regulation on the legal tender of euro banknotes and coins](#); and iii) a proposed [Regulation concerning the provision of digital euro services by payment service providers incorporated in non-euro-area Member States](#). In this paper we focus on Article 33 of the proposed Regulation on the establishment of the digital euro and, more specifically, on access to the hardware and software features of mobile devices needed for online and offline digital euro transactions.

Considerable effort will be required to make the digital euro work effectively. It should become a payment infrastructure that covers all Member States and involves not just the European Central Bank (ECB) but also other relevant stakeholders, including national banks, private companies, merchants and citizens. All of these actors should follow specific principles, standards and processes to ensure interoperability, security and transparency of transactions. Even the apparently technical decisions – such as requirements for interfaces or access procedures – can impact other aspects like competitiveness, operability, and resilience.

It is within this context that Article 33 gains particular importance. Under the proposed Regulation, the ECB and the Eurosystem play a central role in governing the digital euro ecosystem; Article 33 specifically addresses one of its most critical operational dimensions: access to the hardware and software functionalities of mobile devices

required for digital euro payments. Rather than being just a technical provision, Article 33 shapes the wider ecosystem through the conditions it establishes for such access. By doing this, it influences who can effectively provide digital euro services, how competition develops within the ecosystem, and whether control over mobile-device infrastructure can lead to control over access to public digital money.

Specifically, decision-making that aligns with the provisions of this Article will influence the process of ensuring interoperability and security within the payment ecosystem. However, it will also affect other aspects, including division of responsibilities among ecosystem members, access to the new instrument and its evolution along with the European digital economy. Several major questions arise in this regard: Which parts of the ecosystem should be regulated to ensure interoperability and security of payments? What aspects should be left to market-led development and implementation? How should standards be designed to maintain technological neutrality? And what governance processes should be established to achieve these goals?

These issues have become even more important now that the digital euro is emerging as a key component of Europe's strategic infrastructure. Like other critical infrastructures, decision regarding ecosystem governance will determine the payment ecosystem's potential for adaptation, scalability, and resilience. Lack of proper coordination may cause inconsistency and fragmented implementation throughout Member States. Highly prescriptive regulations can, in turn, limit innovation and implementation, thereby hindering the effective functioning of the ecosystem.

Therefore, it is essential to effectively coordinate innovation and standard-setting activities within the digital euro ecosystem. Special attention will be given to three interconnected dimensions of such implementation: the scope and layering of the standard-setting process; the governance mechanisms required for efficient and predictable decision-making; and the implications for access, contestability and single-market compliance.

2. ARTICLE 33 – THE GOVERNANCE HINGE OF THE DIGITAL EURO ECOSYSTEM

While the creation of the digital euro is important, the governance mechanism that will ensure its successful use is equally significant. Each payment system requires a set of common rules to help multiple entities coordinate their activities safely and efficiently. Similarly, the digital euro will need to operate according to specific rules to achieve the same objectives. Although the proposed Regulation established the institutional and regulatory framework for the digital euro, the technical standards that will support its operation have not yet been determined.

Box 1. Article 33 – fair, reasonable and non-discriminatory access to mobile devices

- 1) Without prejudice to Article 6(7) of [Regulation \(EU\) 2022/1925](#), original equipment manufacturers of mobile devices and providers of electronic communications services within the meaning of Article 2(1) of [Directive \(EU\) 2018/1972](#) shall allow providers of front-end services and providers of European Digital Identity Wallets effective interoperability with, and access for the purposes of interoperability to, the hardware features and software features necessary for storing and transferring data to process online or offline digital euro transactions, on fair, reasonable and non-discriminatory terms.
- 2) Original equipment manufacturers of mobile devices and providers of electronic communications services referred to in paragraph 1 shall not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the hardware and software features concerned by the interoperability obligation provided that such measures are duly justified.
- 3) For the purpose of applying fair, reasonable and non-discriminatory terms pursuant to paragraph 1, original equipment manufacturers of mobile devices and providers of electronic communications services referred to in paragraph 1 shall publish general conditions of effective interoperability and access. Such general conditions shall include a European Union-based alternative dispute settlement mechanism. The dispute settlement mechanism shall be without prejudice to the right to seek redress before judicial authorities in accordance with Union and national law.

Source: European Commission, proposal for a Regulation on the establishment of the digital euro, COM(2023) 369 final, Article 33.

Article 33, as proposed by the Commission, does not grant the ECB the authority to adopt technical standards. It establishes an obligation to provide access on fair, reasonable, and non-discriminatory (FRAND) terms, allows strictly necessary, proportionate, and duly justified measures to protect the integrity of the relevant hardware and software, and

requires the publication of general access conditions, including an EU-based alternative dispute resolution mechanism. Both the Council mandate and the European Parliament's negotiating position, discussed below, assign the ECB a role in developing reference standards for secure processing. This addition, which was contested during the parliamentary debate but is now supported by both co-legislators, transforms Article 33 from a provision primarily about access into a broader issue of who sets the standards governing that access. At first glance, this provision appears to be a purely technical rule. On closer inspection, however, it becomes clear that this is an important governance mechanism in the regulatory framework.

Why is that? Standards will help define the terms under which participants in the digital euro ecosystem join the system, process transactions, meet the security requirements and facilitate interoperability across the single market. Standards can affect implementation costs, the implementation process, and the level of innovation and competition within the ecosystem. In other words, decisions about standards will influence the incentive structure, the allocation of responsibility within the ecosystem, and its future development.

This raises another question about the governance of the digital euro: how can we balance central control and decentralised innovation in the digital euro ecosystem? Clearly, not every aspect of the scheme requires standardisation, at least not in full detail. Excessive centralisation can stifle innovation within the ecosystem and impose specific technologies on market participants. However, insufficient coordination can lead to market fragmentation and inconsistencies in implementation and use. How can we find the best approach?

One way to approach this issue is from a multi-layered governance perspective. Different components of the digital euro ecosystem will each have distinct governance characteristics. Some aspects will be necessary for interoperability and will therefore need to be centrally coordinated and standardised, while others are better left to innovation and competition within the market. Table 1 provides a stylised representation of these governance layers, distinguishing between the legislative framework, scheme governance, technical implementation and market-facing services.

Table 1. A layered governance framework for the digital euro ecosystem

Layers	Main actor(s)	Purpose	Examples
Legislative framework	EU legislator (European Parliament and Council)	Establish legal mandate and fundamental rights and obligations	Digital Euro Regulation, legal tender provisions, privacy safeguards, access rights
Scheme governance and rulebook	ECB and Eurosystem	Define common standards necessary for the functioning of the ecosystem	Participation rules, scheme interoperability requirements, security standards, certification procedures, operational rulebook
Technical implementation	PSPs, infrastructure providers, technology providers	Implement standards through operational solutions	Wallet integration, authentication solutions, APIs, connectivity arrangements
Market-facing services and innovation	PSPs, fintechs, banks, merchants	Compete through differentiated services and customer experience	Wallet design, value-added services, budgeting tools, merchant solutions, loyalty programmes

Source: Authors' elaboration.

2.1. THE EVOLVING ROLE OF ARTICLE 33 IN THE LEGISLATIVE NEGOTIATIONS

As the governance role of Article 33 described above shows, it also plays an important part in the ongoing legislative negotiations. As of late July 2026, the Digital Euro Regulation has entered the final stage of the legislative process. The Commission put forward its proposal in June 2023, the [Council adopted its negotiating mandate](#) in December 2025, the [ECON Committee adopted its position](#) on 23 June 2026 (by 43 votes to 14 with one abstention), and the [plenary confirmed the Parliament's negotiating position](#) on 9 July 2026 (by 416 votes to 169 with 22 abstentions), opening the way for trilogue negotiations.

Across the Commission, Council and Parliament texts, Article 33 has become one of the main provisions through which the relationship between access and security is negotiated (i.e. access-security trade-off). Broad access to mobile-device hardware and software can facilitate interoperability and competition, but it may also affect the ability of device providers to control the integrity of security-critical components. Conversely, while safeguards that allow providers to protect their systems may be necessary for security, if these measures are framed too broadly, they could restrict effective access or be applied in a discriminatory manner. The central question, therefore, is how to guarantee effective access while permitting only proportionate and objectively justified security measures.

The Commission proposal established the basic framework for ensuring that all parties have fair, reasonable and non-discriminatory access to the relevant mobile-device hardware and software features. The Council negotiating mandate goes somewhat further by enhancing the overall governance of access conditions, including by adding reference to the development and adoption of common standards, technical specifications and their enforcement. The Parliament's negotiating position goes furthest in this direction: it broadens the set of access beneficiaries, extends the access obligation to functionalities already in use for other digital means of payment, endorses ECB reference standards and Commission implementing acts, and deletes the express security safeguard originally proposed by the Commission.

One element of continuity is easily overlooked. The Commission proposal already empowered the Commission to adopt delegated acts in relation to Article 33 (Articles 5(1) and 38 of the proposal), albeit with little detail as to their content. The Council and Parliament positions replace this approach with more specific implementing powers exercised through comitology. They also introduce the genuinely new element of reference standards, technical specifications and procedures adopted by the ECB. The main differences between the institutional positions are summarised in Table 2.

Table 2. Treatment of Article 33 across the main legislative texts

Issue	Commission proposal (Jun. 2023)	Rapporteur's draft (Nov. 2025)	Council mandate (Dec. 2025)	Parliament position (Jul. 2026)
Access obligation	Requires FRAND access to relevant mobile-device hardware and software features needed for online/offline digital euro transactions	Broadly maintains the Commission approach	Maintains the access obligation, extends it to third-party technical support providers, and specifies that access must not depend on the provider's own services	Maintains and broadens the obligation to cover front-end-service, EUDI Wallet and third-party technical-service providers, as well as functionalities used for other digital means of payment
Security safeguard	Allows device and communication-service providers to take necessary and proportionate	Broadly maintains the Commission approach	Maintains the safeguard, subject to justification	Deletes the express safeguard allowing device and communication-service providers to take necessary and proportionate

	measures to protect integrity			measures to protect hardware and software integrity
ECB reference standards	Not specified in Article 33, although the ECB may adopt detailed measures, rules and standards under its general competences	Does not add a specific Article 33 reference-standards mechanism	Adds ECB reference standards, technical specifications and procedures for secure processing within 6 months	Requires ECB reference standards, technical specifications and procedures within 6 months of authorisation of issuance
Commission powers on access conditions	Article 33 included in delegated-act framework, but with limited detail	Removes Article 33 from the delegated-act list	Adds Commission implementing acts to specify FRAND criteria and implementation measures	Adds Commission implementing acts, with ECB technical assistance, within 6 months of authorisation of issuance
Publication, dispute resolution and enforcement	Requires publication of general access conditions and foresees dispute settlement	Broadly maintains the Commission approach	Strengthens publication, requires EU-based alternative dispute settlement with a 90-day decision period, and gives the Commission a coordination role in enforcement	Requires published access conditions, an EU-based alternative dispute-settlement mechanism and compliance with ECB standards and Commission implementing acts

Source: Authors' elaboration.

This evolution is highly relevant to the argument presented in this paper. Article 33 has moved from being primarily an access provision towards becoming a broader governance provision addressing the relationship between access, security and technical standard-setting. Its immediate subject remains access to the hardware and software features required for digital euro payments. However, the addition of ECB reference standards and Commission implementing powers means that it now also determines how access conditions will be specified and governed.

Article 33 therefore operates principally at the scheme-governance layer identified in Table 1. It does not prescribe the complete technical architecture of the digital euro ecosystem. Instead, it establishes the institutional framework through which common access and interoperability requirements will be translated into standards and

implementation measures. It can consequently be understood as a governance hinge between central coordination and market-led technical implementation.

With the Council and Parliament having formally adopted their negotiating mandates, the trilogue will determine the final outcome. In particular, the Council retains a security safeguard that Parliament has removed, while both institutions assign the ECB and the Commission new roles in implementing Article 33. The treatment of the safeguard, as well as the scope of the ECB reference standards and Commission implementing acts, therefore remain subject for negotiation. This paper examines how these elements can be designed to preserve effective access and interoperability while protecting security, ensuring technological neutrality, and promoting market-driven innovation.

3. WHAT NEEDS TO BE STANDARDISED AND WHAT CAN STAY OPEN?

The success of the digital euro ecosystem will depend not only on having standards but also on their scope. The question of what should be standardised and what should be left to market-driven development is a central question from a governance perspective. On the one hand, too much openness can lead to fragmentation and inconsistent application of standards. On the other hand, excessive standardisation can hinder innovation and lead to unnecessary implementation costs for market participants.

In light of this, the goal of Article 33 should not be maximum standardisation. Instead, the objective should be to establish a minimum common basis necessary for interoperability, security, and resilience, while leaving enough room for innovation. Thus, a tiered approach in which common standards would be developed only for those components that are absolutely necessary for interoperability and security seems advisable. This approach would help to ensure that all the participants in the digital euro ecosystem work according to common principles while leaving implementation choices and service provision mainly to individual entities.

3.1. COMPONENTS OF THE DIGITAL EURO ECOSYSTEM THAT REQUIRE COMMON EUROPEAN STANDARDS

Certain components of the digital euro ecosystem require consistent regulation at the EU level. These components represent the infrastructure layer of the ecosystem and should fall within the main scope of scheme-level governance, whereas Article 33 addresses the device-access dimension.

First, scheme-level interoperability requirements must be standardised. Digital euro payments should flow seamlessly across different intermediaries, Member States and technical platforms. Common standards governing transactions processing, message formats, settlement interaction and communication between scheme participants and the settlement infrastructure are required for that purpose. Without such standards, the digital euro could reproduce the fragmentation it is intended to solve. This is distinct from access to the hardware and software features controlled by mobile devices, which is addressed in Section 4 and should be governed by outcome-based criteria rather than by a prescribed technological architecture.

Second, common security and operational resilience standards need to be developed. At the scheme layer, participants must comply with the same basic security standards in terms of authentication, cybersecurity, anti-fraud measures, business continuity, and incident management. Harmonised minimum standards are essential to maintain trust and stability across the ecosystem. This relates to the security obligations of the parties participating in the scheme. It is distinct from the security of the device environment itself,

which includes the integrity of components such as the Secure Element and the near field communication (NFC) antenna¹. In this context, security should operate as a constraint on access rather than as a basis for prescribing a single technological architecture. This distinction is directly relevant to the trilogue: while the Council retains an explicit security safeguard, that requires justification, Parliament deletes it. The final text should maintain an outcome-based version of that safeguard, allowing device providers to take proportionate and duly justified measures to protect system integrity while still complying with the access requirements outlined in Section 4.

Third, market participants require clear guidelines on certification, compliance, and participation. It is vital for participants to understand the criteria for participating in the digital euro ecosystem, demonstrating compliance, and remaining operationally ready.

Finally, standard management, testing, and introduction of changes need to be under common governance. It is important to understand that the digital euro environment will not remain the same forever. In light of changes in technology, user behaviour, and other market dynamics, certain technical standards and requirements might need to be adjusted.

3.2. AREAS FOR WHICH MARKET-DRIVEN IMPLEMENTATION IS APPROPRIATE

There are some aspects of the digital euro architecture where detailed standardisation is neither necessary nor desirable once interoperability, security and operational consistency are guaranteed. Beyond that common baseline, prescriptive standards may constrain technological choices, increase implementation costs and impede innovation. Market participants should therefore retain sufficient freedom to determine how they implement digital euro services.

Customer interfaces are an obvious candidate. Banks and payment institutions should retain flexibility in designing digital wallets and onboarding procedures, subject to common interoperability, security and accessibility requirements. Interoperability is a necessary condition for adoption, but it is unlikely to differentiate competing payment solutions once the common baseline is met. Consumer choice will also depend on usability, functionality and the overall customer experience.

The same applies to complementary services offered in connection with the digital euro. Budgeting tools, services for merchants, loyalty programmes, linking with other financial

¹ The Secure Element is a tamper-resistant hardware component used to store sensitive payment credentials and cryptographic keys and to execute security-critical payment functions in a protected environment. NFC is the short-range wireless communication technology that enables contactless payments by allowing a mobile device to exchange payment information with a payment terminal.

services, innovative payment options – all of these should stay within the sphere of competition and innovation.

Market participants should retain freedom in implementing technical solutions, provided that the required common outcomes are achieved. Article 33 should specify outcomes – such as effective interoperability, security and non-discriminatory access – rather than prescribe specific technologies or implementation architectures.

This means that not all aspects of the digital euro infrastructure require the same level of standardisation. Some functions must be guaranteed by centralised action in view of their importance to the ecosystem. Other tasks should be entrusted to market participants. Table 3 provides a summary of the suggested division of responsibilities across key areas of the ecosystem.

Table 3. Indicative allocation of standardisation responsibilities within the digital euro ecosystem

Area	Preferred degree of standardisation	Rationale
Scheme interoperability protocols	High	Single market functionality
Access to third-party device functionality	Low (outcome-based)	Technological neutrality; rely on provider process
Scheme security and operational resilience	High	Trust and resilience
Certification and compliance	High	Legal certainty
Wallet design	Low	Innovation and competition
User experience	Low	Consumer choice
Value-added services	Low	Market differentiation
Technical implementation choices	Medium/Low	Technological neutrality

Source: Authors' elaboration.

3.3. PRINCIPLE OF TECHNOLOGICAL NEUTRALITY

The argument outlined above highlights an important governance principle – technological neutrality. Technological neutrality does not mean that there will be no standards at all. What is implied here is that standards should describe what is to be accomplished by participants, but they do not necessarily need to specify how to reach

the goal. This means that the focus should be on the outcomes, such as interoperability, security performance, resiliency requirement and interfaces compatibility, while leaving room for flexible technological implementation strategies.

This principle is especially important for mobile devices, authentication solutions and other technologies that form part of existing digital ecosystems. Prescriptive implementation architectures risk excluding participants, increasing costs, or creating security concerns. In the case of low-level hardware and software features, such as the NFC antenna and the secure element, mandated access can also enlarge the attack surface that the original device security architecture was designed to contain. Security should therefore operate as a constraint on the scope of access, with device providers retaining the ability to take proportionate and justified measures to protect the integrity of their systems. An outcome-oriented approach can support technological developments while preserving interoperability and trust.

As far as Article 33 is concerned, technological neutrality should be viewed as an essential characteristic of the regulatory process. The role of the ECB here is not to choose the specific technological implementation, but rather to ensure the interoperability, security and coherence of various technological solutions across the single market.

Technological neutrality does not, however, by itself guarantee contestability or prevent market concentration. It should be combined with effective and enforceable access obligations, non-discrimination, appropriate oversight and credible dispute settlement. Its role is narrower: to prevent the regulatory framework from unnecessarily favouring or entrenching a particular technological solution.

4. ACCESS, CONTESTABILITY AND IMPLEMENTATION SCALABILITY

Not only will the decisions made in accordance with Article 33 impact issues of interoperability and security, they will also affect who can effectively take part in the digital euro ecosystem. Access therefore constitutes a crucial dimension of digital euro governance. A robust framework that would prove inefficient to implement in the variety of devices, platforms, and infrastructure employed by European consumers would struggle to gain traction and scale up effectively.

This point is especially relevant since digital euro transactions are expected to be conducted widely via mobile devices and digital wallets. In practice, it will mean interactions among payment service providers, operating systems, device manufacturers and authentication systems. Consequently, the governance framework needs to apply to an ecosystem that already has well-established technological architectures, security schemes and distribution mechanisms.

In light of the above, it can be concluded that the purpose of a governance framework is neither to duplicate the existing technological infrastructure nor impose changes on it. Instead the goal should be to ensure that market participants are able to offer digital euro services under fair, predictable and secure access conditions. Such a governance approach requires ensuring contestability without intervening in technological choices which do not impede interoperability or raise security concerns.

For this purpose, Article 33's requirement that access be provided on FRAND terms is central. It requires the entities controlling the relevant mobile-device hardware and software features to provide the effective interoperability and access necessary for digital euro services². They should neither withhold access without objective justification nor impose unreasonable or discriminatory conditions that favour their own services or selected partners. The FRAND requirement therefore operates as a governance tool, ensuring that control over device infrastructure does not become control over which providers can offer digital euro services to users³.

² This does not necessarily require direct access to low-level components, such as the NFC antenna or Secure Element. Access may be provided through a secure, provider-controlled implementation, provided that it enables competing providers to deliver the required core digital euro functionality.

³ The objective of requiring access on FRAND terms under Article 33 is not to guarantee identical technical treatment across all providers. Rather, it is to ensure that competing providers obtain access sufficient to deliver the core functionality required for digital euro services. Providers should remain free to differentiate their interfaces, implementation methods and value-added services. The focus should therefore be on effective access and user capabilities, rather than on a prescribed technical model.

4.1. ARTICLE 33 AND THE DMA: COORDINATION, NOT INCORPORATION

Article 33 operates alongside the [Digital Markets Act](#) (DMA), but it should constitute a self-standing access regime with its own beneficiaries, access conditions, security safeguards and enforcement arrangements⁴. Coordination is necessary where the two regimes overlap, but Article 33 should not import the DMA's regulatory logic or depend on DMA designation. Article 6(7) DMA requires designated gatekeepers to provide providers of services and hardware, free of charge, with effective interoperability with – and access for interoperability purposes to – the operating-system, hardware and software features available to or used by the gatekeeper's own services. This obligation has been applied to certain system-level NFC functionalities. Separately, the [commitments accepted by the Commission in July 2024](#) under Article 102 TFEU, opening NFC functionality to third-party mobile-wallet developers, provides a further example of access being operationalised through competition-law enforcement. Parliament acknowledges this existing framework by making Article 33 applicable without prejudice to Article 6(7) DMA.

The two regimes nevertheless differ in purpose and scope. The DMA obligation applies only to designated gatekeepers, whereas Article 33 applies to original equipment manufacturers of mobile devices and providers of electronic communications services, irrespective of gatekeeper designation. Their beneficiaries also differ. Article 33 covers providers of digital euro user interfaces, EUDI Wallet providers and third-party technical service providers acting on their behalf; Article 6(7) DMA covers providers of services and hardware, as well as business users and alternative providers offering services together with, or in support of, the relevant core platform service. Finally, the DMA requires designated gatekeepers to provide interoperability free of charge, whereas Article 33 requires access on FRAND terms, which does not preclude remuneration.

A key reason for keeping Article 33 self-standing is the risk that its interaction with the DMA could produce different economic conditions for comparable providers. These differences may result in overlapping obligations governing the same mobile-device functionality. A designated gatekeeper may be required to provide particular access free of charge under the DMA, while an entity outside the DMA's scope may be subject only to the FRAND requirement under Article 33. This does not necessarily constitute a formal legal inconsistency: the two instruments have different addressees and policy rationales. This divergence may have competitive as well as technical consequences. Two device providers with similar positions in the EU smartphone market could face different

⁴ The Digital Services Act forms part of the wider EU framework governing digital services and may apply to relevant online intermediary services, including in relation to illegal content, fraudulent advertising and systemic risks. It does not, however, establish an interoperability or mobile-device access regime comparable to Article 6(7) DMA and is therefore not examined further here.

obligations for the same functionality. A provider whose operating system is designated under the DMA could be required to give digital euro service providers free access to system-level functionalities, even where those providers compete with its own payment services. A comparable non-designated provider, by contrast, could charge FRAND terms for the same access. Such differences could arise even where providers offer comparable functionality and face similar security and interoperability requirements. In those circumstances, the applicable economic conditions would turn principally on designation under a separate legal instrument. Depending on how the two regimes interact in practice, Article 33 may therefore result in different economic conditions for comparable device providers and affect competition both between them and between the digital euro services that rely on their devices. This raises questions about the coherence of an Article 33 regime intended to provide access on FRAND terms across all its addressees. This makes it important for the final Regulation to clarify how the obligations interact, including which regime governs the economic and technical conditions of access where both apply.

Parliament's recitals seek to guide that interaction. Recital 69 presents Article 6(7) DMA as applicable to existing and new digital means of payment, including the digital euro. Recital 69a states that the digital euro should be available through functionalities and user interfaces commonly used for comparable digital payments, on FRAND terms – or free of charge where required under the DMA or pursuant to commitments or decisions adopted under Union competition law. It also refers to equivalent conditions and features such as double-click access where available. These recitals indicate Parliament's intended interpretation, but they cannot amend the DMA or resolve all questions concerning its scope. Material requirements governing the interaction between the regimes should therefore be stated clearly in the operative provisions rather than left to recitals, enforcement practice or litigation.

The preceding analysis supports the case for a self-standing Article 33 regime. On this reading, its objective is broader than remedying conduct by designated gatekeepers: it is to ensure that the digital euro can be used across relevant devices regardless of whether the entity controlling the necessary functionality has been designated under the DMA. The reference to Article 6(7) should therefore operate principally as a coordination rule, preserving the application of the DMA where its conditions are met without automatically importing its regulatory logic into Article 33⁵.

⁵ A related issue has arisen in the negotiations on the Financial Data Access Regulation (FiDA), particularly concerning reliance on DMA gatekeeper designation to determine participation in the financial-data framework. See an [ECRI In-Depth Analysis on FiDA](#).

4.2. OUTCOME-BASED ACCESS AND TECHNOLOGICAL NEUTRALITY

Beyond its relationship with the DMA, Article 33 must balance the need for common standards with flexibility in their technical implementation. While the establishment of common standards is essential for ensuring the consistent functioning of digital euro payments throughout the EU, excessively detailed implementation standards might prove counterproductive by increasing implementation costs, reducing flexibility and discouraging market participants from offering their services.

This aspect is especially relevant when considering mobile operating systems, device security systems, and authentication solutions. Indeed, these technologies have been developed in recent years and incorporated into the broader technological ecosystem. Although interoperability requirements might imply common interface standards and security goals, they need not require all technological environments to use a uniform implementation approach.

Thus, the technological neutrality discussed in the previous section has significant relevance for access and contestability as well. Specifically, it is important to ensure fair access conditions to digital euro services while allowing market participants the freedom of choice to choose their preferred implementation approach. In other words, the key requirement is to ensure that digital euro services can be provided consistently across all devices and platforms, whereas the method to reach interoperability and security goals is left flexible.

This would mean assessing the access requirement against outcome-oriented criteria rather than detailed technical specifications. Four criteria are particularly relevant. Access should be timely, so that payment service providers can compete effectively with services offered by the device manufacturer or operating-system provider; technically sufficient to enable developers to build competing digital euro services; non-discriminatory in its terms and practical operation; and any restrictions or conditions should be objectively justified and proportionate to legitimate security, integrity and operational-resilience needs. Proportionality should also apply to the scope and form of the access required, taking account of the operating-system or device provider's intellectual property embodied in the underlying technology without preventing effective access. This criterion-based approach would make the access requirement enforceable while preserving flexibility.

4.3. ACCESS GOVERNANCE, ENFORCEMENT AND SCALABILITY

The legislative negotiations have not yet produced a complete or common enforcement model for Article 33. The Council mandate requires each Member State to designate one or more competent authorities responsible for applying and monitoring Article 33 and to establish penalties for infringements. Parliament's position instead reinforces the roles of the ECB and the Commission in operationalising the access obligation and retains the EU-based alternative dispute-settlement mechanism, but does not establish an equivalent explicit national enforcement structure. The trilogue should therefore clarify not only the content of the access obligation, but also which authorities will monitor compliance, investigate complaints, impose remedies and penalties, and coordinate cases involving more than one Member State or overlaps with the DMA.

The choice of these outcome-oriented criteria has an institutional counterpart that the Regulation should make explicit. The device provider's own access process, through which payment service providers request access to the relevant hardware and software features, should be the primary channel for delivering the required outcome. Prescriptive specification should be held back as a residual backstop, used only where there is documented evidence that the process fails the criteria set out above. This would invert the usual default. It would leave the provider free to design and evolve its process, and to build on standards that already exist, while keeping the most intrusive tool in reserve.

For this arrangement to work, the backstop must nevertheless be credible. If the provider runs the access process, payment service providers may reasonably fear that access could be delayed, refused or granted only on degraded terms. Thus, two conditions must be fulfilled. Firstly, the criteria laid out in Article 33 should be sufficiently clear and legally enforceable, allowing an aggrieved party to use them as a basis for action. Secondly, intervention should be triggered where access is not provided in a timely, technically sufficient or non-discriminatory manner, rather than by a general preference for prescriptive standard-setting.

The assumption that the ECB must necessarily hold such a residual power is not automatically justified. The body in charge of monitoring the access process, assessing the validity of security claims and deciding when this process fails must be sufficiently technically knowledgeable while maintaining impartiality between the parties involved. As the issuer and custodian of the digital euro system, the ECB has a clear interest in ensuring wide access to the functionalities used for making payments using digital euros. That role could create an institutional tension if the ECB were also responsible for resolving disputes concerning the conditions of such access.

Consistent with the objective of creating a self-standing access regime, the backstop should be put into place via the Digital Euro Regulation and apply to all addressees of

Article 33 regardless of their status as gatekeepers. Should Article 33 and the DMA overlap in terms of regulating the access to the same functionalities, the requirement to coordinate the related procedures should be included in order to avoid any conflicting decisions while respecting the jurisdiction of each regime in their respective scope. The backstop itself should be supported by the EU-based alternative dispute-settlement mechanism suggested in the mandate of the Council and negotiating position of Parliament with technical assessments done by an independent institution, if needed.

Parliament's position points partly in this direction. It empowers the Commission, with technical assistance from the ECB, to adopt implementing acts specifying the measures required for effective compliance, while giving the ECB a separate role in adopting reference standards, technical specifications and procedures. These implementing acts establish general compliance measures; they do not themselves resolve individual access disputes. The appropriate division of responsibilities would therefore be for the ECB to define the functional requirements of digital euro access, for the Commission to specify general implementation measures, and for disputes over whether access has been provided on FRAND terms to be considered through a separate and impartial access-governance mechanism.

Finally, one should mention the problem of implementation scalability. The success of digital euro services will depend on the level of participation of intermediary firms, technology companies, and merchants in deploying and integrating those services. Consequently, a governance approach that is predictable and proportionate is more likely to ensure scalability in comparison with a governance framework that forces the re-engineering of existing infrastructures.

5. LESSONS LEARNED FROM CURRENT EUROPEAN SYSTEMS

The issues involved in digital euro governance are not entirely new. There are already many large-scale European payment systems, along with other types of market infrastructures, that require coordinated efforts from various stakeholders, including public authorities, financial institutions, infrastructure providers, and other involved parties. Although the digital euro introduces some unique features, there is much to be learned from how standards have been established and maintained in similar systems.

There are two prominent examples worth mentioning: the [Single Euro Payments Area \(SEPA\)](#) and [TARGET Services](#) by the Eurosystem. In both cases, standards have been combined with decentralised implementation and provide valuable lessons for digital euro standards.

5.1. SEPA: STANDARDISED APPROACH, DECENTRALISED IMPLEMENTATION

SEPA is an initiative meant to introduce a [common framework](#) for euro payments in Europe. It has been successful due to the clear division between common requirements and decentralised competitive approaches for meeting them. Payment schemes, messaging standards, and general requirements have been defined centrally; however, financial institutions and payment service companies have the freedom to choose the specific services and ways for delivering them to customers.

One distinctive element of SEPA has been its governance process. The technical and operational standards were created following industry governance processes involving market consultation and transparent management of changes. This has facilitated interoperability and allowed for evolution and adaptation to changes in the market.

In the case of the digital euro, it seems reasonable to conclude that interoperability does not have to be achieved through homogeneity in the implementation approach. Common standards and competition can work side by side provided the line between them is clearly drawn.

5.2. TARGET SERVICES: OPERATIONAL GOVERNANCE AND RESILIENCE

The Eurosystem's TARGET Services represent a second good example. These infrastructures play an important role in the functioning of financial markets and thus demand consistent operation across all participants. Therefore, operational governance should pay special attention to security, business continuity and change management.

What is interesting about TARGET governance is the existence of structures in which users and stakeholders participate in the development and adjustment of such arrangements.

This makes it possible to combine the practicality of solutions with their conceptual coherence.

An excellent illustration of this is the governance model for [TARGET2-Securities \(T2S\)](#). In order to support the introduction of securities settlements activities within Europe, there was much cooperation among the stakeholders, as well as testing processes and phases of implementation. Although T2S cannot be directly compared to a digital euro because it deals with security rather than retail payments, it gives some ideas about the discipline required when implementing common standards.

As far as the digital euro is concerned, the most valuable lesson that could be learned from this model is the need to combine centralised decision-making and stakeholder participation in it. The governance model, which does not take account of operational conditions, might make the implementation of Article 33 difficult, expensive, or inefficient.

Although SEPA and TARGET have somewhat different goals, they both show how standards, operational arrangements, and participation can be arranged in a pan-European ecosystem. The main elements of such governance are listed in Table 4.

Table 4. Governance features of existing European payment infrastructures and their relevance for the digital euro

Governance feature	SEPA	TARGET Services	Relevance for the digital euro
Common rulebook	✓	✓	Essential
Stakeholder consultation	✓	✓	Essential
Change management procedures	✓	✓	Essential
Technical standard-setting	✓	✓	Essential
Decentralised implementation	✓	Partial	Important
Scope for differentiated implementation	High	More limited	Important

Source: Authors' elaboration.

5.3. IMPLICATIONS FOR THE GOVERNANCE OF THE DIGITAL EURO

The experience of SEPA and TARGET suggests that an effective approach to governance would be one that combines central coordination with structured stakeholder participation. Either a fully centralised decision-making process or an approach based exclusively on market-driven standardisation may, if applied alone, prove insufficient for a pan-European public payment system.

Thus, the governance structure of the digital euro should distinguish between scheme-level standard-setting and device-level access. At the scheme level, the ECB should set and oversee the common standards, while ensuring structured participation by market stakeholders in their development and modification. In contrast, when it comes to access to mobile-device functionality, the obligation should define outcomes rather than prescribe the system architecture. Any residual power to intervene should rest with a body selected for its technical expertise and impartiality, rather than with the ECB in its role as the issuer of the digital euro. This approach would promote transparency, accountability, proportionality, technological neutrality and operational feasibility.

As was highlighted by the SEPA and TARGET examples, the central lesson running throughout this paper is that governance should not prescribe how objectives are implemented, but should focus on outcomes, common requirements and shared goals.

6. OPERATIONAL GOVERNANCE FOR THE DIGITAL EURO

The analysis in this paper highlights that the success of the digital euro will be depend less on the existence of standards and more on the way they are governed. The proposed framework provides the basis for organising the standards, access conditions and operational arrangements required for implementation. The objective now is to build an operational framework based on this mandate that promotes interoperability and resilience while maintaining the potential for innovation, contestability and scalable implementation.

The analysis points towards a framework build on six complementary pillars. These pillars together aim to ensure a proper balance between interoperability, resilience and legal certainty on one side, and innovation, contestability and operational scalability on the other side. Table 5 provides the details of this framework.

Table 5. Pillars of an operational governance framework for the digital euro

Governance pillar	Objective
Layered standard-setting	Interoperability without over-standardisation
Technological neutrality	Flexibility and future-proofing
Structured stakeholder participation	Technical expertise, security, legitimacy and operational feasibility
Change management	Predictability and adaptability
Single-market consistency	Scalability and integration
Self-standing and coordinated access regime	Secure, consistent and enforceable access conditions

Source: Authors' elaboration.

The first pillar is a layered approach to standard-setting. Standards should be set primarily in areas that require consistency for the proper functioning of the pan-European payment infrastructure, specifically in interoperability, security, certification and resilience. On the other hand, customer-facing services, implementation decisions and added-value functionality should be kept open for further innovation driven by the market. This approach would promote both efficiency and flexibility within the ecosystem over the long term.

The second pillar is technological neutrality. As outlined above, standards should define outcomes without prescribing a specific implementation architecture, as doing so would

create potential risks of technological lock-in and hamper the coexistence of different solutions within a shared ecosystem.

The third pillar is structured stakeholder participation. Governance should combine central coordination with the direct participation of stakeholders expected to implement, operate or be materially affected by the relevant standards. Participation should be tailored to the subject matter: payment service providers, infrastructure providers, device manufacturers, operating-system providers, wallet providers, merchants, consumer representatives and security experts should be involved where their activities or systems are affected. Participation should begin early and continue through consultation, technical working groups, testing and change management, while remaining transparent and balanced and without giving any category of stakeholder a veto over the final outcome.

The fourth pillar is predictable change management. The digital euro ecosystem will inevitably evolve in response to technological developments, changing user preferences and new market conditions. Governance arrangements should therefore include clear and structured procedures for consultation, testing, certification, implementation and transition whenever standards are modified. Predictability is particularly important for participants that must make long-term investments in infrastructure, compliance and operational capabilities. The Parliament's negotiating position reinforces this pillar by requiring pilot testing in a controlled real-life environment before the first issuance, a roll-out phase of at least 24 months and a public announcement of the planned issuance date at least 2 years in advance.

The fifth pillar is single-market consistency combined with space for innovation. One of the primary goals of the digital euro is to establish a truly European payment system. Therefore, governance principles should promote consistency with minimal fragmentation caused by different national implementation approaches, while preserving competition and innovation in areas that do not impact interoperability, security, and resilience.

The sixth pillar is a self-standing and coordinated access regime. First, the final Regulation should include an outcome-based security safeguard. Device and OS vendors must be allowed to take necessary, proportionate, and justified measures to secure their systems, while being required to provide non-discriminatory and effective access. This means that security will be recognised as a legitimate ground for restricting the method of access, but not as a general basis for denying effective access.

Second, Article 33 should establish its own beneficiaries, access conditions, safeguards and enforcement arrangements for all its addressees, irrespective of whether they are

designated as gatekeepers under the DMA. This does not mean displacing the DMA in cases where Article 6(7) applies. It means that the Digital Euro Regulation should not rely on DMA designation to determine the content of its own access regime. Because the DMA and Article 33 differ in scope and economic conditions – including free access under the DMA and access on FRAND terms under Article 33 – the final Regulation should clarify how the two regimes interact where both cover the same functionality. Procedural coordination should preserve each regime within its own scope and prevent inconsistent decisions or unnecessary differences in implementation.

Access governance also requires an appropriate separation of functions. The ECB should define the functional outcomes and reference standards required for the digital euro, while the Commission should specify general implementation measures. The Article 33 backstop and dispute-settlement mechanism should be established within the Digital Euro Regulation, cover all Article 33 addressees and be supported by independent technical assessment.

Overall, the main elements mentioned above present governance principles that entail central coordination, technological neutrality and involvement of stakeholders in the decision-making process. This approach will allow the ECB to perform its duties under Article 33 while making sure that the digital euro ecosystem will be open, contestable and scalable.

7. CONCLUSIONS

The discussion about the digital euro is shifting from principles to implementation. As the project develops, its successful implementation will depend not only on the relevant legal framework and necessary technical capabilities, but also on how the digital euro ecosystem operates.

This paper argues that Article 33 should not be seen merely as a tool for standard-setting. First of all, this provision governs access to mobile devices, and its conditions will help determine which participants in the digital euro ecosystem can offer their payment services. Therefore, the decisions under Article 33 will not only influence the functioning of the system, but will also impact its attractiveness, contestability, innovation capability and scalability.

Effective governance requires correct balancing between the role of the central coordinating authority and market actors' freedom to act and implement various solutions. In some areas, such as interoperability, security, certification and operational resilience, a consistent set of scheme-level rules and standards across the single market are absolutely essential. However, in other areas, such as innovation, customer experience and implementation aspects, the freedom to compete for the best solution should be left to market participants. Access to the functionality of mobile devices is an area where maintaining this balance is especially important. Therefore, the regulatory framework should set the goals that must be achieved through access, rather than dictating particular technological designs. At the same time, it should permit necessary, proportionate and duly justified measures to protect system integrity while maintaining effective access. Prescriptive regulation should be used only when these goals cannot be achieved in any other way.

Finally, the Regulation should establish a standalone Article 33 access regime applicable to the addressees, while ensuring coordination with the DMA when the same functionality is regulated. The ECB should set the functional requirements and the reference standards necessary for the digital euro, the Commission – the general implementation measures, while individual disputes concerning access conditions should be decided through an impartial mechanism supported by independent technical expertise.

The trilogue will now determine this institutional and substantive balance. Among the main issues is the security safeguard deleted by the Parliament but maintained by the Council, the scope of ECB reference standards and implementing acts adopted by the Commission, and the interaction between Article 33 and Article 6(7) DMA.

The main issue, however, is not the necessity for the standards themselves but the design and governance of the standard-setting process, as well as their implementation and modification. The framework based on layered standard-setting, technological neutrality, structured involvement of stakeholders in the decision-making process, predictable change management, single-market consistency and secure and enforceable access regime can provide the basis for an open, competitive and scalable digital euro ecosystem.



CEPS
PLACE DU CONGRES 1
B-1000 BRUSSELS
