



EU RegCORE Client Alert

Financial Services

October 2026



Dr. Michael Huertas

Tel: +49 160 97375760

michael.huertas@pwc.com

Dr. Hagen Weiss

Tel: +49 1511 5708446

hagen.weiss@pwc.com

**Fabian Joshua Schmidt,
LL.M.**

Tel: +49 151 41490437

fabian.jos-

hua.schmidt@pwc.com

EU RegCORE Team

de_regcore@pwc.com

From Pool to Payment: Building End-to-End On- Chain Securitisation in Europe

The EU has assembled several of the regulatory and infrastructure components necessary to support tokenised securitisation. Comparable developments in the United Kingdom create opportunities for interoperability, although the EU and UK legal frameworks remain distinct; this Client Alert focuses on EU and German law issues and notes the principal UK divergences. The commercial question is whether these components can be connected across the transaction lifecycle: from origination and asset transfer through issuance, settlement, servicing, reporting and redemption. A tokenised note alone does not achieve that connection. A genuinely end-to-end model must also determine which events produce the intended legal effects, and which remain subject to off-chain verification and decision-making.¹

¹ Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation [2017] OJ L 347/35 (**SECR**); Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology [2022] OJ L 151/1 (**DLTPR**); Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998

DLT can alter the infrastructure through which a securitisation operates; it does not, by itself, change the requirements for legal effectiveness. A ledger entry may provide evidence, constitute an agreed instruction or, where legislation so provides, form part of a legally effective registration or transfer. Its consequences depend on applicable law, the authoritative register and transaction documents. Technical consensus alone is not an assignment, perfection step, discharge of an obligation, proprietary transfer or statutory settlement finality. This separation between execution and legal consequence governs the analysis below.

Several developments now make the distinction commercially important. Pontes has entered operation for eligible wholesale settlement; the securitisation framework is under review; the Commission has proposed widening the DLT Pilot Regime and modernising settlement-finality legislation. These independent workstreams could progressively enable a more connected securitisation lifecycle, but neither their adoption nor their availability to any particular transaction should be assumed.

The relevant question therefore is no longer simply whether an asset-backed security can be tokenised. It is whether the securitisation itself can become programmable from pool to payment – and, if so, which parts of the transaction remain irreducibly legal. This alert sets out the lifecycle, identifies the legal control point at each stage, and offers a realistic assessment of what can move on-chain now and what cannot.²

Why this matters now

On 21 September 2026, the Eurosystem launched Pontes, allowing eligible wholesale tokenised-asset transactions to settle in central bank money by connecting participating DLT market infrastructures with TARGET Services. The initial launch offers a core set of services, with participant onboarding and functionality developing progressively through 2028. Pontes does not itself automate borrower collections, waterfall distributions, coupon payments or redemptions. The tokenisation of the underlying exposures and the wider securitisation value chain was also the subject of the panel “Tokenisation in Securitisation – Underlying Assets, Value Chain and Digital Euro” at the TSI Congress on 2 October 2026, in which the authors participated. The panel title provides a useful lens for this Client Alert; no particular statement or consensus is attributed to its participants.³

Four developments converging

1. **Pontes is operational.** Since 21 September 2026, supported wholesale transactions in tokenised assets can settle in central bank money through eligible participating infrastructures. This supplies a significant component of the potential cash leg, but access, transaction coverage, participant eligibility and available functionality remain conditional. Borrower payments, asset purchases, note subscriptions and subsequent distributions must each be analysed separately.

on settlement finality in payment and securities settlement systems [1998] OJ L 166/45 (**Settlement Finality Directive**); Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements [2002] OJ L 168/43 (**Financial Collateral Directive**); Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets [2023] OJ L 150/40 (**MiCAR**). The expression *on-chain securitisation* is used in this alert descriptively, to denote a securitisation whose lifecycle events are recorded and in part executed through distributed-ledger infrastructure. It is not a defined term in EU law and is not the title of any legislative instrument.

² This alert describes legislative proposals and policy workstreams that are not yet law. The SECR review, the MISP amendments to the DLTPR and the proposed Settlement Finality Regulation are each subject to the ordinary legislative procedure and may change materially before adoption. Nothing in this alert should be read as a statement of the law as currently in force.

³European Central Bank, “Eurosystem brings central bank money to tokenised finance” (21 September 2026).

- 2. **The EU securitisation framework is under review.** Following the Commission proposals of 17 June 2025, the Council adopted its negotiating position on 19 December 2025 and Parliament confirmed its decision to enter interinstitutional negotiations on 21 May 2026. The package addresses transparency, investor due diligence, risk retention and the prudential treatment of securitisation exposures. It is not a tokenisation initiative; its eventual provisions will nevertheless shape the legal and economic conditions for digital transactions.
- 3. **The DLT Pilot Regime may be widened.** The Commission’s Market Integration and Supervision Package (**MISP**) of 4 December 2025 proposes broader eligibility for financial instruments and a EUR 100 billion aggregate market-value limit for instruments admitted to trading or recorded on a DLT market infrastructure. A differentiated simplified arrangement for eligible smaller infrastructures providing relevant CSD services is proposed with a EUR 10 billion threshold, subject to applicable conditions. These proposed measures could address one constraint on structured-finance scale without resolving custody, liquidity, distribution or cross-border property-law questions.⁴
- 4. **Settlement finality is being modernised.** The MISP includes a proposal to replace the Settlement Finality Directive with a directly applicable Settlement Finality Regulation and to amend the Financial Collateral Directive. For tokenised securities, the key inquiry is whether a transaction takes place in an arrangement benefiting from statutory protection and at what point the applicable rules treat the relevant instruction as irrevocable and final. Ledger consensus is not equivalent to insolvency-protected settlement finality.⁵

Individually, none of these developments creates an on-chain securitisation. Together they change the question that firms should be asking. It is no longer whether an asset-backed security can be tokenised. It is: *Can the securitisation itself become programmable from pool to payment?*

At a glance: what an end-to-end on-chain securitisation could look like

The table below illustrates a traditional securitisation involving the transfer of underlying exposures to a securitisation special purpose entity (**SSPE**) and the issuance of asset-backed securities (**ABS**). Synthetic securitisations may instead transfer credit risk through guarantees or credit derivatives without transferring the underlying claims; their legal control points differ. The figure maps potential digital capabilities and does not imply that any particular infrastructure presently performs every stage.⁶

Stage	Lifecycle event	Digital layer
1. <i>Origination</i>	Loans, mortgages or receivables are created	Digital asset identity and authenticated servicing data

⁴European Commission, Market Integration and Supervision Package (4 December 2025), including COM(2025) 943 final and proposed amendments to Regulation (EU) 2022/858. The proposed EUR 100 billion and EUR 10 billion frameworks have distinct conditions and remain subject to negotiation.

⁵European Commission, Market Integration and Supervision Package (4 December 2025), proposed Settlement Finality Regulation and related amendments to Directive 2002/47/EC; see https://finance.ec.europa.eu/publications/market-integration-and-supervision-package_en. Legislative proposals only.

⁶ Figure 1 is an illustrative description of a possible lifecycle architecture prepared for this Client Alert. It is not a forecast of market practice, nor a description of any existing transaction or infrastructure.

Stage	Lifecycle event	Digital layer
2. Pool creation	Eligibility criteria and concentration tests are applied	Automated pool-selection and monitoring logic
3. Asset / risk transfer	Transfer from originator to SSPE	Legal assignment and perfection, with digital confirmation of transfer status
4. Securitisation issuance	SSPE issues senior, mezzanine and junior notes	Native DLT financial instruments, or digital representation of conventional securities
5. Primary settlement	Exchange of investor cash against securities	Delivery-versus-payment, potentially central-bank-money settlement through Pontes
6. Servicing / oracle layer	Borrower payments, arrears, defaults and recoveries	Authenticated off-chain data transmitted into transaction infrastructure
7. Waterfall	Interest, principal, reserves and triggers	Deterministic calculations executed through programmable logic
8. Regulatory and investor reporting	Article 7 disclosures, investor reports and repository data	A single authoritative dataset feeding multiple outputs
9. Secondary market	Trading, custody, transfer and collateral use	DLT trading and settlement infrastructure with legally recognised finality
10. Redemption / default	Maturity, clean-up call, acceleration or enforcement	Final payment, cancellation of the securities and legally governed close-out

The most important point is that the chain is not purely technological. At every stage there is a legal control point – a step at which the intended consequence depends on something other than the correct operation of the code. Those control points, not the ledger design, determine whether a transaction works.

The legal control points

The following table compresses the lifecycle into the question that technology answers and the question that it does not. It is deliberately asymmetric: the second column describes capability, the third describes the legal determination that must still be made by someone, under some law, in some document.⁷

Lifecycle stage	What technology can do	Legal question that remains
Origination	Create a trusted digital asset identity	What legally constitutes the underlying claim?
Pooling	Test eligibility automatically	Are the eligibility criteria correctly reflected in the code?
Transfer	Record movement from originator to SSPE	Has legal title actually transferred and been perfected?

⁷ The table below is analytical rather than prescriptive. The legal questions in the third column are indicative and will differ by asset class, governing law and transaction structure.

Lifecycle stage	What technology can do	Legal question that remains
Issuance	Create native digital securities	What constitutes the authoritative ownership record?
Subscription	Effect an atomic exchange of cash and securities	When are the payment and the securities transfer final?
Servicing	Feed asset-performance data into the system	Who validates off-chain events and corrects errors?
Waterfall	Automate deterministic calculations	Which decisions require contractual discretion?
Reporting	Generate investor and regulatory datasets	Who remains legally responsible for Article 7 compliance?
Secondary trading	Transfer securities rapidly	Are transfer, custody and investor restrictions satisfied?
Default	Execute predefined responses	Who determines default and exercises enforcement discretion?

The distinction between technological execution and legal effectiveness is the foundation of any credible on-chain securitisation model. A transaction that automates the first while leaving the second undocumented has not become more efficient. It has merely moved its unresolved questions into the code. The sections that follow trace that distinction through each stage of the lifecycle, beginning with what separates an on-chain securitisation from a tokenised note.

1. Moving beyond the tokenised note

There is an important difference between a tokenised securitisation and an on-chain securitisation. In the first model, an otherwise conventional securitisation closes using existing origination, transfer, servicing and reporting processes, and only the securities issued by the SSPE are represented on DLT. That can already produce benefits in issuance, settlement, custody and transferability. It does not fundamentally change the transaction.

An end-to-end model goes considerably further. The relevant state of the underlying exposures – ownership, payments, eligibility criteria, concentration limits, credit events and waterfall calculations – could increasingly be represented digitally and connected to the securities themselves. The transaction then starts to resemble a continuously updating operating system rather than a collection of periodically reconciled databases. That is where the larger efficiencies sit, and it is also where the legal work becomes materially harder.

2. The underlying assets: bringing the pool on-chain

Once the end-to-end ambition is accepted, the first layer to address is not the security but the pool. For mortgages, auto loans, SME loans, consumer receivables or other financial assets, a functioning system needs trusted information concerning each exposure: outstanding principal, accrued interest, payment status, arrears, prepayments, defaults, restructurings and recoveries. DLT could provide a shared data layer through which authorised participants obtain a consistent version of that information, and smart-contract logic could then test eligibility criteria and concentration limits automatically. A loan that ceased satisfying a revolving-period eligibility criterion could, for example, be identified as the relevant state changes rather than during a subsequent manual reconciliation.

The legal asset must be distinguished from its digital representation. The validity of an assignment between the parties, its effect against the borrower, its priority against third-party claims and its enforceability in insolvency require separate analysis under the relevant contractual, property, conflicts and insolvency rules. Notification, consent or registration may be necessary depending on the assets and jurisdictions. A DLT identifier or ownership status should be updated as legally conclusive only after the applicable transfer requirements have been verified. The discussion at the 2026 TSI Congress similarly framed tokenisation as an issue extending to underlying assets and the value chain, rather than only the securities issued.⁸

Nor should personal borrower data be entered indiscriminately onto an immutable ledger. Permissioned access, pseudonymisation and hashing do not automatically remove information from the GDPR: re-identification, lawful processing, controller and processor allocation, data retention, international transfers and data-subject rights, including the tension between the right to erasure under Article 17 GDPR and ledger immutability, require assessment. Banking secrecy and confidentiality obligations owed to borrowers must be assessed alongside the GDPR. In many structures, personal information should remain off-chain, subject to controlled access, while authenticated identifiers and status confirmations support shared processing.

3. True sale cannot simply be coded

Bringing the pool on-chain leads directly to the question of transfer. In a traditional true-sale securitisation, separation of the underlying exposures from originator insolvency risk requires legally effective sale or assignment arrangements and careful consideration of debtor defences, perfection, set-off, commingling, re-characterisation and clawback. This is distinct from the wider assessment of the SSPE's insolvency remoteness, including corporate purpose, limited recourse, non-petition, account control and continuity of servicing. A synthetic securitisation presents different legal requirements: enforceable credit protection and, where relevant, the prudential recognition of significant risk transfer. None of these consequences follows automatically from recording an event on DLT.

In a synthetic securitisation, the relevant control points include enforceability of credit protection, verification of credit events, determination of losses and protection payments, and where applicable collateral arrangements. Automated portfolio monitoring cannot replace the prudential conditions governing significant risk transfer under the CRR or any relevant supervisory assessment. Equally, tokenised issuance does not establish simple, transparent and standardised (**STS**) status, which must be assessed against the applicable SECR criteria.

What DLT can change is the evidence and execution surrounding that process. A transaction could increasingly connect eligible asset, transfer instruction, perfection status, purchase-price payment, SSPE ownership record and securitisation funding into a single traceable sequence. For revolving transactions, the same infrastructure could monitor additions, substitutions and removals from the pool as they occur. This could materially improve the audit trail between asset eligibility, asset transfer and funding – an area where conventional transactions still rely heavily on periodic certification. But the smart contract should execute the legal agreement. It should not become an untested substitute for it.

4. Native issuance rather than digital wrapping

⁸ The true-sale criteria in Article 20 SECR apply only to STS securitisations; SECR otherwise does not itself prescribe how underlying exposures are transferred, although its risk-retention requirements apply generally. Whether an assignment is effective against the debtor and third parties, and whether it survives the insolvency of the originator, remains a matter for the applicable national property, contract and insolvency law.

Once the assets have been validly transferred to the SSPE, the next control point is the form of the securities it issues. A token representing an interest in a conventionally issued security must be distinguished from a security constituted electronically under an applicable statutory framework. Germany's Electronic Securities Act (*Gesetz über elektronische Wertpapiere*, **eWpG**)⁹ provides an established (EU Member State anchored) example. For instruments within eWpG's scope, including bearer debt securities, entry in an electronic securities register replaces the issuance of a physical certificate. Subject to the Act's specific provisions, the resulting electronic security has the same legal effect as its certificated equivalent. For qualifying debt securities, registration may take place in a central register or a crypto-securities register: an eWpG issuance is therefore not necessarily a blockchain issuance.

The distinction between individual and collective registration is equally important. For individually registered electronic securities, §§ 24 and 25 eWpG connect legally effective dispositions and transfers of ownership to the relevant register acts, alongside the other statutory requirements. Ownership transfer requires agreement and re-registration on the entitled person's instruction. Collective registration instead engages the co-ownership and custody arrangements addressed by § 9. A technical movement between wallet addresses must therefore be assessed against the applicable registration and holding model; it cannot automatically be treated as a legally effective transfer of the investor's entitlement.

German practice has also progressed beyond the isolated issuance of a digital instrument. In March 2026, a legally binding pilot involving a bank as issuer and KfW as investor demonstrated a programmable bond workflow under the eWpG. Its report¹⁰ describes connected issuance terms, automated ISIN allocation, crypto-securities registration and delivery-versus-payment settlement, including processes for coupon payments and redemption. Settlement linked the securities infrastructure to central bank money in T2 through the Bundesbank's Trigger Solution. However, the pilot retained manual steps and an off-chain interface to the registrar. It demonstrates a legally constituted bond workflow, not the elimination of every operational dependency or the general availability of a production service.

A separate development concerns continuity during the life of an outstanding security. On 23 September 2026, KfW changed the registrar of its third crypto bond and moved the register between two DLT infrastructures. This provides a practical example of infrastructure migration during a bond's term. It does not establish unrestricted cross-chain portability, and a planned migration should not be confused with recovery from an unexpected platform failure or the insolvency of a service provider.

For securitisation, the conclusion is important but bounded. These transactions demonstrate capabilities at the securities and settlement layers; they do not themselves evidence the integrated transfer of a securitisation portfolio, verification of borrower collections, operation of a tranching waterfall and satisfaction of the transaction's reporting obligations. The question is consequently no longer whether German law can support a legally effective digital note. It is how those established securities-law mechanisms and demonstrated operating processes can be connected to the distinct legal and operational arrangements governing the underlying assets, servicing, cash management and investor reporting.

DLT does not determine an instrument's regulatory classification. Where a tokenised securitisation note qualifies as a financial instrument under MiFID II, it falls outside MiCAR by virtue of Article 2(4)(a). Its issuance, placement, trading, settlement and custody instead engage the applicable securities-markets

⁹ Gesetz über elektronische Wertpapiere (eWpG) vom 3. Juni 2021 (BGBl. I S. 1423), as amended, in particular §§ 1–4, 8–9, 16–18 and 24–25. For individually registered electronic securities, § 25(1) requires agreement concerning the transfer of ownership and re-registration on the instruction of the entitled person. Collective registration is governed by a different statutory and custody-law structure.

¹⁰ *Smart Bond Contract: Disintermediating the Life Cycle of a Tokenized Security — Pilot Report* (March 2026), pp. 1–6, particularly section 4.5, section 7 and the disclaimer on p. 6. The report distinguishes the executed pilot workflow from further contemplated automation and general production availability.

framework, including MiFID II/MiFIR, CSDR, the DLTPR where relevant, SECR and national securities law. Any separate settlement token or payment instrument requires its own classification.¹¹

MISP's proposed DLTPR expansion would remove existing product-specific eligibility thresholds, broaden access for financial instruments and increase the aggregate permitted market value to EUR 100 billion. The proposed EUR 10 billion simplified framework for certain smaller infrastructures is not a general exemption for all operators. Any expansion remains subject to legislative agreement and the relevant authorisation, investor-protection, settlement and operational conditions. The reforms could support scalability, but legal recognition, distribution and liquidity remain separate constraints.

The availability of eWpG issuance must also be separated from eligibility under the DLTPR. Article 3(1)(b) of the existing regime excludes debt instruments with embedded derivatives or structures that make their risks difficult for clients to understand. A proposed tokenised securitisation cannot therefore be treated as eligible merely because its notes are validly issued under the eWpG or fall below a numerical threshold. The instrument's characteristics and the proposed infrastructure must be assessed separately. DLT-based arrangements outside the Pilot Regime may also be considered, but must comply with the ordinarily applicable securities and market-infrastructure requirements rather than assume the availability of Pilot exemptions.¹²

Where any part of the transaction is governed by English law or involves UK investors or infrastructure, the analysis diverges. The DLTPR, MiCAR, the proposed Settlement Finality Regulation and Pontes do not apply in the United Kingdom. The relevant UK framework instead includes the Securitisation Regulations 2024 together with the FCA and PRA securitisation rules, the Digital Securities Sandbox, and the Financial Markets and Insolvency (Settlement Finality) Regulations 1999. Under English law, a legal assignment of receivables under section 136 of the Law of Property Act 1925 requires written notice to the debtor, so securitisations commonly rely on equitable assignment with notice deferred until a perfection event; a digital transfer status must reflect that distinction. The Property (Digital Assets etc) Act 2025 confirms that digital assets may attract personal property rights, but it does not by itself determine the effect of a ledger entry on title to the underlying receivables or to the notes.

5. The cash leg may be the decisive breakthrough

Legally constituted digital notes deliver limited benefit unless they can be settled against cash. A persistent challenge for tokenised securities is the connection between the asset leg and the cash leg. Pontes now makes wholesale central-bank-money settlement available to supported DLT transactions through participating infrastructure, but does not itself link every payment in a securitisation. Borrower collections, servicer remittances, asset-purchase consideration, subscription proceeds, secondary trades, coupons and principal repayments represent different legal obligations and may involve different eligible participants and settlement arrangements.

The ECB announced on 21 September 2026 that it had begun preparatory work to invest a limited portion of its own-funds portfolio in tokenised securities with settlement through Pontes. The initial focus is euro-denominated euro-area public-sector and European supranational instruments, not securitisation notes.

¹¹Regulation (EU) 2023/1114 (MiCAR), Article 2(4)(a); Directive 2014/65/EU (MiFID II), Article 4(1)(15) and Annex I Section C; Regulation (EU) 2022/858; national securities legislation including the German eWpG.

¹² Regulation (EU) 2022/858 [2022] OJ L 151/1, Article 3(1)(b) and recital 7. Instrument eligibility under the Pilot Regime must be distinguished from the legal constitution of an electronic security under national law and from the provision of DLT-based services in compliance with the ordinary regulatory framework.

This is evidence of growing institutional engagement with the infrastructure rather than completed securitisation deployment.¹³

The payment chain must therefore be analysed as several distinct cash legs rather than one uninterrupted settlement event. Borrower payments, servicer remittances, transaction-account movements, investor subscriptions and noteholder distributions may involve different settlement assets, intermediaries, rules on availability of funds and moments of legal discharge. In particular, a digital euro should not be presented as presently available for retail borrower collections into securitisation structures.

Project Agorá offers a complementary example: BIS-led prototype work and controlled testing have demonstrated the feasibility of arrangements involving tokenised commercial-bank deposits and central-bank reserves across currencies. This is not yet a generally accessible production settlement service for securitisations. Nor should wholesale central-bank-money settlement through Pontes be confused with the proposed digital euro, which addresses a distinct, principally retail payment use case. Central-bank money, commercial-bank money, tokenised deposits and e-money tokens have different legal, liquidity, credit and finality implications. The digital-money theme of the TSI Congress panel accordingly highlights the need to map which form of money can settle each obligation rather than assuming a single cash token can support the whole lifecycle.¹⁴

6. The waterfall is an obvious potential candidate for automation

Once the cash legs have been mapped, the allocation of those funds among noteholders becomes the natural focus. A securitisation waterfall contains many rules capable of deterministic calculation, including interest, principal, fees, reserves, quantitative triggers, note balances and payment-date amounts. Programmable logic can improve calculation and the audit trail, but the determination of an amount due must be separated from authorisation and execution of the corresponding payment. Funds must be available under the transaction documents, required approvals must be obtained and completion must be reconciled against the relevant account and settlement records. The precise order of payments remains transaction-specific.

That does not mean every provision should be automated. Other provisions require judgement. A servicer, trustee, security trustee, calculation agent, originator or the noteholders may need to determine whether an event of default has occurred, waive a breach, replace a counterparty, amend documents or pursue enforcement. Those are not deterministic functions dressed up as discretionary ones; they are genuinely evaluative decisions with legal consequences. The stronger model is therefore not a completely autonomous securitisation. It is a legally governed programmable securitisation, in which deterministic functions are automated and discretion remains allocated to identifiable decision-makers.

7. The servicer becomes the critical oracle

An automated waterfall, however, is only as reliable as the data that feeds it. One of the most underestimated components of on-chain securitisation is the servicer. Most borrowers will not make payments directly into the DLT environment supporting the securities. A consumer-loan borrower may simply transfer a monthly instalment of EUR 450 from an ordinary current account. Something must tell the transaction infrastructure that the payment occurred. That makes the integrity of the oracle layer central rather than peripheral.

¹³European Central Bank, "ECB to invest part of own funds in tokenised securities, with settlement via Pontes" (21 September 2026):

¹⁴Bank for International Settlements, "Project Agorá shows how tokenisation can improve wholesale cross-border payments" (27 May 2026); prototype and controlled tests do not constitute general production availability.

The transaction therefore needs rules identifying who submits and authenticates servicing information, when a data point becomes authoritative, how corrections work and who can suspend automated processing. It must distinguish a borrower's payment instruction from receipt by the servicer and from amounts finally available to the SSPE. Reversals, chargebacks, commingling and servicer insolvency could otherwise cause a digital state to overstate distributable cash. Insolvency, a moratorium, repossession or enforceable recovery also requires an authorised determination of the off-chain legal event.

Data governance consequently becomes a transaction-law issue. Servicing agreements and associated technology arrangements should address verification standards, reconciliation, audit rights, incident procedures, continuity, replacement and dispute resolution. Where the institution and relevant ICT services fall within DORA, the applicable ICT third-party requirements should be separately assessed; outsourcing or servicing is not automatically an ICT service within that regime.

8. Article 7 reporting could move closer to event-driven, single-source reporting

The same authenticated servicing data that drives the waterfall also underpins the transaction's disclosure obligations. Article 7 SECR requires specified information concerning underlying exposures, transaction documentation, investor reporting and material events to be made available in accordance with the Regulation. Responsibility must be allocated among the originator, sponsor and SSPE, including designation of the entity fulfilling the relevant information requirements. The prescribed formats, channels, frequency and access arrangements continue to apply, with differences depending on the transaction. A digital common dataset can support rather than displace those legal obligations.¹⁵

The opportunity is to maintain a controlled, authoritative transaction dataset capable of producing consistent investor, repository and supervisory outputs at the applicable reporting dates and upon relevant events. This is distinct from imposing continuous reporting where the law does not require it. It may reduce reconciliation costs and improve data quality, but an eventual shift towards direct supervisory access would require a separate legal basis, appropriate governance and infrastructure. In this sense, regulation by infrastructure means using the architecture that operates the transaction to generate reliable compliance information.

9. From reporting to a Regulatory Digital Twin

Taken a step further, a single authoritative dataset could support more than periodic reports. A "Regulatory Digital Twin" would represent the legally and operationally relevant state of a securitisation: pool composition, exposures, note balances, cash flows, triggers and contractual priorities. It should not be treated as an autonomous legal register or a substitute for supervisory submissions. Each data point should be traceable to its authoritative source, and any provisional or contested legal event should retain that status until validly determined. Such an architecture could support controlled, more timely supervisory insight without purporting to confer new supervisory access powers.

That does not mean supervisors should receive borrower-level personal data or unrestricted access to commercial information. Access would require governance, proportionality, cybersecurity and confidentiality controls, and those controls are part of the design rather than an afterthought. But conceptually the supervisory model could move from periodic reporting of historic states towards controlled access to continuously

¹⁵Regulation (EU) 2017/2402 (SECR), Article 7(1)–(2), including designation of the entity responsible for fulfilling the prescribed information requirements; applicable regulatory technical and implementing standards.

generated regulatory states. That is “Digital Prudential Supervision” applied to structured finance. Securitisation may be unusually well suited to it, because the product already depends heavily on highly structured data, pre-defined contractual rules and extensive reporting.

10. The secondary market needs the same infrastructure

Primary-market and reporting efficiencies will be of limited value if the securities cannot subsequently be traded and settled with equivalent legal certainty. Issuing an asset-backed security token without a functioning secondary market only solves part of the problem. Institutional adoption requires trading access, custody, wallet infrastructure, investor eligibility controls, transfer restrictions, delivery-versus-payment, recordkeeping, collateral eligibility and legally effective settlement finality. The MISP is relevant precisely because it seeks to expand the DLTPR and facilitate greater scale in DLT trading and settlement.¹⁶

MISP’s proposal for a Settlement Finality Regulation and related Financial Collateral Directive amendments may affect the legal framework for DLT settlement. Technical settlement, proprietary transfer and statutory insolvency-protected finality remain separate questions. The analysis must identify the relevant designated system or protected arrangement, its rules, participants, applicable law, timing of irrevocability and discharge, and the scope of insolvency protection. A token’s movement alone does not resolve those matters.¹⁷¹⁸

11. End-to-end does not mean everything sits on one chain

A common misconception is that successful tokenisation requires every element of the transaction to exist on a single blockchain. That is neither necessary nor necessarily desirable. A credible institutional architecture is much more likely to consist of interoperable layers, each doing what it is suited to do, with defined interfaces between them. Figure 2 sets out a minimum viable architecture on that basis.¹⁹

Layer	Content	Where it sits
Origination system	Borrower documentation, KYC, loan agreement and payment history	Mostly off-chain
Asset data / digital twin layer	Digital identifiers, balances, status and eligibility information	Permissioned, shared infrastructure
Legal transfer layer	Sale agreement, assignment, perfection and true-sale analysis	Legal documentation with digitally recorded state
SSPE / issuance layer	Senior, mezzanine and junior securities	Potentially native DLT securities
Cash / settlement layer	Subscription and secondary settlement	Pontes, a qualifying commercial-bank-money solution or another permitted settlement asset
Servicing / oracle layer	Borrower payments, defaults, recoveries and amendments	Off-chain event converted into an authenticated digital state

¹⁶ See n 6 above.

¹⁷ See n 7 above.

¹⁸ For tokenised securitisation the point is not academic: the moment at which a transfer becomes final, irrevocable and protected against insolvency effects is determined by the settlement-finality framework and the applicable insolvency law, not by the consensus mechanism of the ledger.

¹⁹ See n 8 above.

Layer	Content	Where it sits
Programmable transaction layer	Waterfall, triggers, reserve accounts and calculations	Automation where the rules are deterministic
Reporting layer	Investors, securitisation repository and competent authorities	Generated from common authoritative data
Secondary-market layer	Trading, settlement, custody and collateral use	DLT infrastructure interacting with conventional markets

Interoperability requires more than messaging between ledgers. Origination systems, registers, servicers, account banks, custodians and settlement operators must allocate authoritative-source responsibilities, validation rules, interface failure risk and dispute resolution. Authenticated transmission does not ensure that each system attributes the same legal effect to an event. A multi-layer model should therefore be supported by enforceable contractual and technical interfaces.

12. What can realistically move on-chain now

Against that layered architecture, the practical question is which functions can be digitalised today. The table separates functions technically capable of substantial digitalisation, activities still requiring off-chain verification or legal acts, and capabilities whose broad deployment depends on infrastructure or legal development. This classification describes possibilities, not universal present availability: actual implementation depends on the asset class, governing law, authorisations, participants, market-infrastructure access and operational controls. Automated preparation of regulatory data must also be distinguished from legally compliant disclosure and submission.

Capable of substantial digitalisation now	Partial digitalisation, still requiring legal or off-chain processes	Dependent on further infrastructure or legal development
Loan-level data; eligibility testing; concentration tests; transaction-state monitoring; native digital securities where permitted; subscription processes; certain settlement processes; deterministic waterfall calculations; investor reporting; transaction audit trails.	Transfer of the underlying receivables; perfection; borrower notifications; servicing; default determination; collateral enforcement; discretionary waivers; document amendments; insolvency processes.	Seamless cross-border recognition of digital transfers; universal institutional custody; fully interoperable DLT markets; broad collateral eligibility; widely available cross-platform atomic settlement across heterogeneous infrastructures; harmonised treatment of digital proprietary rights; continuous supervisory access.

The German experience shows why these categories should be treated as an implementation map rather than a simple progression from legally unavailable to legally available. Particular digital-securities and settlement functions can already be combined within defined arrangements, while broader deployment still depends on participant access, legal eligibility and operational integration. The first column identifies potential efficiency gains, not guaranteed savings. The second requires both transaction-specific legal analysis and reliable interfaces to off-chain processes; documentation and technology must work together. The third identifies constraints on wider deployment, rather than establishing that every individual use case must await new legislation. A credible first transaction should therefore assemble the functions available to its participants and test the resulting legal, operational and economic outcomes.

13. A practical first transaction

Applying that implementation map to a concrete structure illustrates how the pieces might fit together. The first commercially credible institutional transaction is likely to be hybrid. Consider an illustrative EUR 500 million portfolio of consumer loans supporting senior, mezzanine and junior securities, alongside any necessary credit enhancement, reserve and liquidity arrangements. The loan purchase price, note proceeds, retained interests and fees must be reconciled in the transaction's sources and uses. Loans would be transferred to the SSPE through enforceable assignment documentation, with transfer and perfection status reflected in a permissioned digital environment only after verification. This arrangement does not depend upon the ledger itself creating the legal assignment.

For an institution considering a first transaction, the business case should compare the existing model against the digital alternative in terms of setup expenditure, ongoing infrastructure charges, investor reach, transaction liquidity, error reduction and reporting efficiency. Custody eligibility, ratings and prudential capital outcomes must be tested alongside technical functionality; none follows automatically from tokenisation.

For illustration, the SSPE might issue EUR 400 million senior, EUR 75 million mezzanine and EUR 25 million junior notes, subject to the transaction's actual structural and commercial requirements. Because the notes in this simplified example equal the portfolio balance, any reserve fund, liquidity support, overcollateralisation or purchase-price discount would require separate funding, for example through a subordinated loan. If the originator retained the entire junior tranche, this could satisfy the first-loss retention option under Article 6(3)(d) SECR, since the junior notes represent 5% of the securitised exposures; the retention method must nonetheless be confirmed against the final structure. Where legally and operationally supported, securities might be issued natively in electronic form and settled against investor cash through eligible delivery-versus-payment infrastructure, potentially using Pontes where the relevant market infrastructure and participants are admitted. The servicer would subsequently provide authenticated information on collections, arrears, prepayments, defaults and recoveries.

For a German-law implementation, the notes could in principle be structured as electronic bearer debt securities under the eWpG, subject to the applicable issuance, registration, custody and distribution requirements. The documents would need to identify the statutory register, the individual or collective holding model and the respective functions of the registrar, custodian and transaction agents. Maintaining a crypto-securities register is itself a financial service requiring BaFin authorisation under the German Banking Act (KWG), which affects the choice of registrar and any later migration. The electronic-securities register would establish the relevant securities record; it would not itself effect the SSPE's acquisition of the underlying consumer loans. Where German assignment law applies, that acquisition would continue to require an effective assignment under the applicable rules.

Nor should the eWpG be described as wholly irrelevant to the payment side of the notes. Its provisions also address rights under electronic debt securities, issuer defences and performance mechanics. The structuring exercise must therefore connect the contractual waterfall and payment arrangements to the rights embodied in the notes and the applicable register procedures. In particular, redemption should reconcile the amount contractually due, completed payment and the required securities-register actions. Cancellation or burning of a token should not, without that legal and payment analysis, be treated as proof that the issuer's obligations have been discharged.²⁰

The infrastructure could then calculate available revenue and principal funds, expenses, interest, reserve and liquidity requirements, triggers, principal allocations and residual distributions in accordance with the

²⁰ eWpG, §§ 28–29, concerning rights under electronically issued debt securities, issuer defences and performance; see also §§ 1–2, 8–9 and 24–25 for the issuance and holding arrangements. For assignment of the underlying receivables where German law applies, see § 398 BGB and the other applicable assignment requirements.

transaction-specific priority of payments. After the required contractual checks and authorisations, it could generate payment instructions for the relevant banking or settlement systems. The same controlled dataset could produce investor and regulatory outputs. Its success would be measured against processing, reconciliation and compliance costs, alongside investor acceptance, credit-rating considerations, liquidity and transaction resilience.

Fallback arrangements should separately address an operational platform failure, a dispute about a proprietary or contractual record, and the insolvency or replacement of an essential counterparty. The appropriate response may include suspension, authoritative-state recovery, migration, contractual step-in or formal enforcement, with clear approval responsibilities and reconciliations before operation resumes.

14. What happens when something goes wrong

A well-designed first transaction must also be tested against failure. The most difficult test of tokenisation is not the performing transaction. It is the broken one. Assume that servicing data is wrong; that a waterfall calculation produces an unexpected result; that the servicer becomes insolvent; that a smart contract contains an error; that the DLT platform becomes unavailable; that a transfer is recorded digitally but is legally ineffective; that a noteholder loses access credentials; or that an event of default occurs. A transaction designed only for the happy path is not institutional infrastructure.

The documentation therefore needs a digital fallback architecture, addressing the hierarchy between code and contract, authoritative records, error correction, suspension rights, emergency intervention, replacement service providers, technology migration, business continuity, key loss, cyber incidents, dispute resolution and enforcement. Each of those is a drafting question before it is a technology question, and none of them can sensibly be resolved after closing.

The KfW migration also illustrates why infrastructure continuity requires legal as well as technical design. The original tokens were not transferred directly between the two DLT infrastructures: replacement tokens were created on the destination infrastructure and the corresponding tokens on the original infrastructure were subsequently deleted through a coordinated process. For a securitisation, such a process would need controls preserving the continuity of investor rights, preventing duplicate representations and reconciling the relevant records before normal processing resumed.

Changing the register operator must also be distinguished from transferring a crypto security to another electronic securities register. Section 16(2) eWpG generally permits an issuer to change the registrar without the consent of the holder (*Inhaber*) or entitled person (*Berechtigter*) unless the issuance terms provide otherwise. Section 22 separately sets consent requirements for a transfer to another electronic securities register; the precise consent and approval route should be confirmed against the statutory text for each transaction. Because the KfW process involved the creation of replacement tokens and the prior consent of the collectively registered holder, documentation should state expressly which statutory route is relied upon and whether any consent is obtained as a legal requirement or as a precaution. A migration clause must therefore identify the contemplated change, the applicable approval route and any additional contractual requirements, rather than assuming that a general technology-replacement provision authorises every form of migration.²¹

²¹ eWpG, § 16(2), concerning a change of registrar, and § 22, concerning transfer to another electronic securities register. See also KfW, *Rigorous test for KfW's third blockchain bond: Lessons Learned* (24 September 2026), pp. 1–3, describing prior consent from the collectively registered holder, transfer of register data, creation of replacement tokens and subsequent deletion of the original tokens.

Rather than establish a universal ranking of law, transaction documents, statutory register and code, the transaction must specify the legal and evidential function of each. Mandatory law and statutory registration rules determine certain consequences regardless of contractual drafting. Subject to those rules, documentation should identify authoritative records, controlling contractual terms, permitted instructions, error correction, suspension and recovery procedures. Disputed proprietary rights and insolvency effects cannot necessarily be settled through a private hierarchy of records.

15. Pontes today, Appia tomorrow

The resilience of any such structure also depends on the public infrastructure on which it relies. Pontes provides an operational bridge between eligible DLT market activity and central-bank-money settlement through TARGET Services, with features and access expanding incrementally. Appia addresses longer-term architecture, governance, standardisation and interoperability for tokenised European financial markets. The Eurosystem published the Appia roadmap in March 2026 and envisages a blueprint in 2028. They are complementary programmes, not guarantees of universal market accessibility.²²

The two initiatives ask different questions. Pontes asks how tokenised markets can access central bank money now. Appia asks what Europe's future tokenised financial market architecture should look like. End-to-end securitisation sits directly at the intersection of those questions, because it requires both an operational settlement asset today and a coherent market architecture tomorrow.

16. The larger prize: from product innovation to market architecture

Viewed together, these infrastructure programmes point beyond individual products. The larger opportunity is to reduce the number of separately maintained transaction states while preserving enforceability and accountability. Delivering that outcome requires common data standards, credible custodial and settlement arrangements, reliable servicing inputs, resilient technology and contractual interfaces. The benchmark is not how much of the transaction is recorded on DLT, but whether the arrangement reduces cost, improves control, strengthens investor information and produces effective legal outcomes.

For originators, arrangers and investors, the decisive question is whether operational improvements outweigh legal structuring, infrastructure, custody, systems integration, assurance, rating, ongoing governance and liquidity costs. An instrument may be technically capable of tokenisation yet economically unattractive if institutional distribution channels are limited or investors require an additional liquidity or technology-risk premium. This implementation test should inform pilots before costly platform decisions are made.

Practical considerations for firms

The developments described above are proposals and infrastructure programmes rather than settled law, and firms should accordingly use them as a design stress test rather than a compliance deadline. The table below sets out, by stakeholder, the questions that are worth answering now – in most cases because the answers will shape documentation and system design long before any legislative text is final.

²²European Central Bank, "Eurosystem unveils Appia roadmap for Europe's tokenised finance" (11 March 2026), <https://www.ecb.europa.eu/press/pr/date/2026/html/ecb.pr260311~14ddf51a77.en.html>; blueprint envisaged for 2028.

Stakeholder	Key points
If you are an originator or bank	- Identify the asset classes whose ownership, servicing data and cash flows can be represented reliably in digital form; granular and standardised pools are likely to provide stronger initial use cases than highly bespoke assets. - Map which components of current securitisation processes represent genuine legal requirements and which exist primarily because institutions maintain separate systems. - Treat those two categories as distinct: only the second is available for elimination through shared infrastructure.
If you are an arranger or issuer	- Begin designing documentation capable of supporting both conventional and DLT execution. - Answer expressly: which register is authoritative; what constitutes transfer of the security; how executable logic interacts with the terms and conditions; who controls upgrades; how coding errors are corrected; what happens during an outage; and whether the transaction can migrate to another infrastructure.
If you are an investor	- Expect due diligence to expand beyond credit and structural analysis to protocol governance, smart-contract risk, custody arrangements, wallet architecture, key management, oracle dependency, data integrity, interoperability and digital business continuity. - Tokenisation does not reduce the importance of due diligence. It expands its perimeter.
If you are a servicer, trustee or agent	- Expect these roles to change significantly rather than disappear; automation can eliminate repetitive processing while increasing the importance of control functions. - The party responsible for verifying information, controlling cash, exercising discretion or resolving inconsistencies may become more important precisely because routine processes have been automated.
If you operate market infrastructure	- The largest commercial opportunity may ultimately sit at infrastructure level rather than at instrument level. - The winner may not be the firm that produces the most sophisticated asset-backed security token, but the infrastructure that connects origination, transfer, issuance, settlement, servicing, reporting and secondary liquidity while remaining legally interoperable throughout the EU and, where relevant, with the UK.

Beyond firm-specific considerations, a number of legislative and infrastructure developments will determine how quickly any of this becomes practicable.

What to watch next

- **SECR trilogues.** The Council agreed its negotiating position in December 2025 and the European Parliament authorised interinstitutional negotiations in May 2026. The outcome will set the transparency, due-diligence and risk-retention architecture within which any digital securitisation must operate.
- **MISP and the DLT Pilot Regime.** Watch the negotiation of eligibility for all financial instruments, the increase of the aggregate market-value cap to EUR 100 billion and the proposed simplified regime below EUR 10 billion. These thresholds will significantly affect whether DLTPR infrastructure can carry

structured-finance volumes, although DLT-based arrangements under the ordinary regulatory framework remain an alternative.

- **Settlement finality and financial collateral.** The proposed Settlement Finality Regulation and the accompanying amendments to the Financial Collateral Directive remain in the ordinary legislative procedure. Their final form will determine whether, and from when, transfer orders in qualifying DLT arrangements benefit from statutory finality protection against insolvency effects; proprietary and wider insolvency-law questions will remain for applicable national law.
- **Pontes connections and the ECB's own funds.** The practical question is how quickly market infrastructures and banks connect real issuance, collateral and settlement flows to Pontes. The ECB's preparatory work to invest part of its own funds in tokenised securities settled via Pontes is an early indicator.
- **The Appia blueprint.** The Eurosystem's roadmap published in March 2026 is expected to culminate in 2028 with the blueprint for an integrated European tokenised financial ecosystem.
- **Project Agorá.** The prototype combining tokenised commercial-bank deposits and central-bank reserves on a programmable platform, with atomic wholesale settlement across currencies, indicates what a multi-currency cash leg might eventually look like.
- **Private-law recognition of digital transfers.** The pace at which Member States recognise the proprietary effects of digital transfers will determine whether a cross-border tokenised securitisation can achieve the same legal outcome in each relevant jurisdiction. This is the slowest-moving component and potentially the most decisive.

Taken together, these workstreams are beginning to supply the architecture that end-to-end on-chain securitisation would require.

Outlook

Europe's emerging tokenised-finance infrastructure creates an opportunity for securitisation to move beyond digitised instruments towards more connected transactions. However, the SECR review, proposed DLTPR and finality reforms, Pontes and Appia address different elements, proceed on different timelines and do not themselves establish an end-to-end legal solution. The discussion at the TSI Congress on 2 October 2026 aptly brought together underlying assets, the value chain and digital money: success depends on enforceable connections between these elements.²³

The practical question is how far originators, issuers, investors and infrastructures can replace serial reconciliations with reliably governed shared data and controlled execution. This requires a structure-specific assessment of asset transfer or credit protection, issuance, cash control, servicing, settlement, reporting, prudential treatment, technology continuity and insolvency outcomes. The resulting Regulatory Digital Twin

²³ No particular statement or consensus is attributed to the panel participants.

would remain a supervised representation of the transaction, not a substitute for the instruments and laws that determine legal rights.

Near-term progress should be judged by measurable reductions in reconciliation, error rates, time to report and transaction costs, without compromising legal certainty, investor protection, regulatory compliance or secondary liquidity. Firms capable of combining those elements may help redesign European securitisation infrastructure; issuing a token alone will not deliver that result.



About us

PwC Legal supports financial institutions, originators, arrangers, investors and market-infrastructure providers in evaluating tokenised financial-market arrangements, including securitisation structuring, digital-securities issuance, settlement, custody, transaction documentation, reporting, technology governance, operational resilience and supervisory engagement. Such projects require an integrated assessment of legal effectiveness, market access, transaction economics and the practical allocation of responsibility.

Moreover, we have developed a number of RegTech and SupTech tools for supervised firms, including PwC Legal's Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from multiple thousands of legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Equally, in leveraging our Rule Scanner technology, we offer a further solution for clients to digitise financial services firms' relevant internal policies and procedures, create a comprehensive documentation inventory with an established documentation hierarchy and embedded glossary that has version control over a defined backward plus forward looking timeline to be able to ensure changes in one policy are carried through over to other policy and procedure documents, critical path dependencies are mapped and legislative and regulatory developments are flagged where these may require actions to be taken in such policies and procedures.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award" and the "2025 Regulatory, Governance and Compliance Technology Award".

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our [website](#).



Contact

Dr. Michael Huertas

Tel: +49 160 97375760

michael.huertas@pwc.com

Fabian Joshua Schmidt, LL.M.

Tel: +49 151 41490437

fabian.joshua.schmidt@pwc.com

Dr. Hagen Weiss

Tel: +49 1511 5708446

hagen.weiss@pwc.com

EU RegCORE Team

de_regcore@pwc.com

