

DIGITALTRADE4.EU, RIHO VEDLER

Proposal and Comment Information

Title: Implementing the Federal Reserve Board's Responsibilities under the GENIUS Act, R-1899

Comment ID: FR-2026-0033-01-C17

Submitter Information

Organization Name: DigitalTrade4.EU

Organization Type: Foreign

Name: Riho Vedler

Submitted Date: 10/09/2026

DigitalTrade4.EU supports a technology-neutral, risk-based implementation of the GENIUS Act that enables innovation in payment stablecoins while ensuring legal certainty, transparency, security and regulatory accountability.

Our feedback recommends strengthening oversight of tokenised reserve assets, third-party dependencies, smart contracts and cross-chain interoperability. The key message is that interoperability must preserve legal rights, verifiable information, compliance obligations and auditability—not merely technical connectivity.

We advocate proportionate, evidence-based controls, privacy-preserving compliance, reliable fraud prevention and operational safeguards that ensure continuity even when technology providers or systems fail. The objective is to support innovation without compromising financial stability, consumer protection or regulatory responsibility.

Comments on the Federal Reserve Board's Proposed Rule Implementing the GENIUS Act

DigitalTrade4.EU

Contact: Riho Vedler | secretariat@digitaltrade4.eu | October 2026 | v5

Abstract. This submission responds selectively to Docket No. R-1899, the Federal Reserve Board's proposed rule implementing its responsibilities under the GENIUS Act. DigitalTrade4.EU supports a technology-neutral, risk-based framework that preserves the legal and operational responsibilities of Board-supervised permitted payment stablecoin issuers while allowing innovation in tokenised reserve assets, programmable execution and interoperability. The submission focuses on proposed § 247.13 and Questions 124–131 and 249–251, including third-party tokenisation, smart contracts, blockchain and cross-chain risks, data privacy, tokenised reserve assets, interoperability, BSA/AML and sanctions controls, and fraud. It recommends a source-and-evidence approach that distinguishes an authoritative legal or operational source, its technical representation, verification evidence, compliance outcomes and the regulated decision that follows. It also proposes a compact supervisory dependency profile, materiality-based testing and implementation examples. The objective is not to prescribe a common ledger or database, but to ensure that material dependencies remain attributable, current, auditable, portable and operationally usable, including during provider failure, state correction or cross-chain transition.

KEY WORDS. payment stablecoins; GENIUS Act; interoperability; tokenised reserve assets; third-party risk; BSA/AML; sanctions; evidence lineage; programmable settlement.

1. Introduction

The Federal Reserve Board's proposed rule under Docket No. R-1899 is an important step from statutory design to operational supervision of payment stablecoin issuers. The proposal addresses permissible activities, reserve assets, redemption, risk management, information technology and security, audits and reporting, capital, custody and related matters for Board-supervised permitted payment stablecoin issuers (PPSIs). It also asks detailed questions about technology, tokenised reserve assets, third-party relationships, cross-chain transfers and interoperability. DigitalTrade4.EU limits this response to those questions for which its prior work on digital-trade interoperability, payment transparency, verified evidence and institutional digital finance provides a directly relevant basis.

The submission does not propose that the Board adopt a specific ledger, token standard, identity framework, trust registry or digital-trade architecture. Nor does it seek to alter the statutory allocation of responsibility under the GENIUS Act, the Bank Secrecy Act, sanctions law or other applicable United States law. Its narrower proposition is that technology-neutral

rules can be made more operationally precise by distinguishing the legal or operational source on which a regulated function depends from a technical representation of that source, from evidence that a verification occurred, from a compliance outcome and from the regulated decision or transaction that follows.¹

This distinction becomes especially important where a PPSI relies on third parties to tokenise reserve assets, maintain smart-contract code, safeguard private keys, provide blockchain monitoring, operate cross-chain bridges or resolve identity and compliance information. The Board itself recognises that such relationships may be material to safety and soundness and proposes due diligence, contractual controls and ongoing monitoring. DigitalTrade4.EU supports that direction and recommends that the final rule or supervisory guidance make the dependency itself more observable: who maintains the authoritative state, what legal claim the token represents, which version or status is current, how corrections or revocations propagate, what service is permitted to attest, and what fallback applies if a provider is unavailable or returns a stale or inconsistent state.¹

The same logic applies to interoperability. Compatibility between blockchains or message formats does not by itself establish legal, semantic or compliance interoperability. A bridge can move or represent a token while leaving unresolved whether the destination representation carries the same legal claim, whether required compliance information remains linked to the transfer, whether a redemption obligation can still be discharged, or whether a corrected upstream state is visible to the relying institution. The appropriate regulatory objective is therefore not maximum technical connectivity. It is controlled interoperability that preserves legal meaning, accountability, traceability and operational continuity.

This approach is consistent with DigitalTrade4.EU's separate submissions on FATF Recommendation 16, MiCA and third-party dependencies in financial market infrastructures. Those materials distinguish underlying regulated information from credentials, proofs, references and derived compliance outcomes; distinguish technical representation from legal effect; and recommend function-level mapping of authoritative sources, third-party outputs and fallback paths. They are cited here as conceptual support only. They are not U.S. law and are not presented as adopted Federal Reserve, FATF, CPMI-IOSCO or European standards.²³⁴

For that reason, this response concentrates on Questions 124–131 and 249–251. The principal regulatory anchors are proposed § 247.13(a)(5) on third-party relationships; proposed § 247.13(b) on information technology and security; proposed § 247.13(c) on enterprise-wide risk management; proposed § 247.13(d), which addresses BSA/AML and sanctions requirements; and section 12 of the GENIUS Act (12 U.S.C. 5912) on compatibility and interoperability. The response also treats the Act's self-executing requirement that a PPSI have the technological capability to comply with lawful orders, 12 U.S.C. 5903(a)(6)(B), as a relevant cross-cutting implementation constraint.¹ The recommendations are principles-based and intended to remain usable across public, permissioned and hybrid ledgers, conventional databases, tokenised and non-tokenised reserve assets, and different technical models for payment stablecoin issuance and circulation. Each response also states the subject of the Board's question so that the substantive mapping remains clear if Federal Register pagination or editorial numbering differs from the draft notice.

2. Executive Summary

1. **Dependency lineage and prevailing source.** For every dependency material to issuance, reserve integrity, redemption, custody or mandatory compliance, the PPSI should be able to identify the authoritative legal or operational source, the technical representation relied upon, the responsible provider, the current version/status, and the

fallback path. Where technical and authoritative states diverge, the PPSI should follow a documented prevailing-source and divergent-state protocol rather than infer legal effect from a ledger entry alone.

2. **Minimum interoperability profile.** Interoperability under 12 U.S.C. 5912 should be evaluated by continuity of identity, legal claim, compliance information, audit evidence and fallback semantics—not by connectivity alone. A bridge, message converter or token wrapper should not sever the link between the issuer, the relevant claim, the regulated institution’s BSA/AML and sanctions responsibilities, and the evidence needed to reconstruct the transaction.
3. **Lawful-order and degraded-state capability.** Consistent with 12 U.S.C. 5903(a)(6)(B), PPSIs should design issuance, redemption and supported-network arrangements so that an unmanaged external dependency does not make compliance with a lawful order operationally impossible. For material bridges, tokenisation layers and smart contracts, pre-defined circuit breakers, operational holds, alternate redemption paths, reconciliation steps and evidence-preservation procedures should be tested for outages and for stale, corrected, revoked or inconsistent states.
4. **Materiality-based scaling.** Controls should scale with the dependency’s consequence for a regulated outcome. Enhanced lifecycle, change, resilience and third-party controls are most justified where a dependency can affect minting or burning, reserve eligibility or availability, redemption, custody, sanctions/BSA-AML gating or lawful-order execution. Advisory, display or non-critical routing functions should not automatically receive the same treatment.
5. **Supervisory usability and fraud resilience.** The Board can operationalise these principles through non-prescriptive examination examples and a compact dependency profile showing source, provider, authority, version/status, transaction binding, fallback and audit evidence. Authenticity controls should also address ecosystem fraud—including issuer impersonation, spoofed wallet or bridge interfaces, fake endpoints and fabricated compliance attestations—and require the PPSI to suspend reliance on a material representation when authenticity or current authority cannot be established.

Table 1. Selected R-1899 regulatory anchors and response focus.

R-1899 anchor	Issue addressed	DigitalTrade4.EU contribution
Proposed § 247.13(a)(5); Q125	Third-party relationships and tokenised reserve assets	Map legal claim, authoritative record, provider role, lifecycle, reconciliation, fallback and audit evidence.
Proposed § 247.13(b); Q126–130	IT/security, smart contracts, blockchain, privacy and tokenised reserves	Use lifecycle and current-state controls proportionate to whether the technology is material to issuance, reserve integrity, redemption, custody or compliance.
Proposed § 247.13(c); Q131	Enterprise-wide risk management	Permit consolidated controls, but require explicit stablecoin-specific dependency mapping and testing.

Proposed § 247.13(d)	BSA/AML and sanctions	Preserve the distinction between required underlying information, verification evidence, analytics outputs and accountable compliance decisions; keep information usable across interoperability steps.
GENIUS Act § 12, 12 U.S.C. 5912; Q249–250	Compatibility and interoperability	Define interoperability by continuity of identity, claim, compliance, audit and fallback semantics rather than technical connectivity alone.
12 U.S.C. 5903(a)(6)(B)	Technological capability to comply with lawful orders	Ensure critical technical dependencies support authorised freeze, restriction, investigation, recovery or other lawful actions without obscuring responsibility.
Q251	Fraud and token authenticity	Bind authenticity to the legal issuer and authorised technical representation, with machine-readable change and revocation semantics.
Q125, Q127, Q130; 12 U.S.C. 5903(a)(6)(B)	Divergent states, degraded operation and lawful-order capability	Use prevailing-source rules, exception states, circuit breakers/holds, controlled fallback, reconciliation and evidence preservation without assuming every external ledger action is reversible.

3. Cross-Cutting Design Principles

Legal and economic substance before technical representation—A tokenised reserve asset should be analysed first by reference to the underlying legal claim, custody arrangement, redemption or transfer rights and applicable law. Tokenisation may change operational risks and control points, but should not be assumed to change the legal nature of an otherwise unchanged asset. Conversely, a technically identical token can embody different legal rights depending on the issuer, custodian, governing law and authoritative record. The final framework should therefore avoid using technical form as a proxy for legal effect.

Authoritative source, representation and evidence—For material regulated functions, the PPSI should document which source is authoritative for the relevant state. A DLT entry, credential, bridge message, oracle output, index or cryptographic proof may provide strong evidence, but it is not necessarily the authoritative legal or operational source. Where the technical representation and the authoritative source can diverge, the arrangement should specify a prevailing-source rule, correction and reconciliation procedure, and the effect on pending and completed transactions.

Current-state usability—Availability should mean more than endpoint uptime. A service can be reachable while returning a stale, revoked, superseded, mismatched or legally unusable state. Material third-party services should therefore be assessed for current-state validity, permitted reliance, latency appropriate to the regulated process and the ability to reconstruct historical decisions.

Accountability through automation—Smart contracts, automated compliance engines and AI-assisted analytics may reduce latency and improve consistency, but their output should remain traceable to the inputs, version and responsible institutional decision. Automation should

not obscure which entity is responsible for minting, burning, redemption, reserve integrity, sanctions controls or another regulated act.

Brownfield interoperability—Interoperability requirements should assume that PPSIs will interact with existing banks, custodians, payment infrastructures, identity providers, reserve-asset systems and multiple blockchain environments. A sound framework should therefore support governed interfaces between heterogeneous systems rather than assume migration to a single ledger or common database.

International context (non-binding)—DigitalTrade4.EU’s earlier FATF Recommendation 16 and MiCA work is cited only as comparative implementation material illustrating recurring technical problems such as information continuity, source/evidence separation and technology-neutral classification. It is not offered as a source of U.S. legal obligations, and this submission does not recommend importing EU classifications, FATF terminology or foreign supervisory structures into Regulation UU. The operative legal anchors for these comments are the GENIUS Act, proposed part 247 and applicable U.S. BSA/AML and sanctions requirements.

4. Responses to Risk-Management and Technology Questions

Question 124 - Scope of risk management—DigitalTrade4.EU considers proposed § 247.13 appropriately broad as a foundation, but recommends that supervisory implementation expressly recognise information-state and dependency risks where a PPSI relies on external digital infrastructure. The relevant risk is not limited to vendor outage. It includes reliance on an output that is stale, incorrectly attributed, no longer legally effective, bound to the wrong transaction, generated from a superseded source state, or operationally inaccessible within the required decision window.

For material digital-asset-service-provider activities, the Board could expect a PPSI to maintain a function-level dependency record identifying: the regulated function; the authoritative source or system of record; the third-party service or transformation; the required output; the downstream consumer; the current status or version semantics; material failure modes; and the fallback or stop condition. This can be incorporated into existing third-party and operational-risk frameworks rather than established as a separate new risk taxonomy.

Question 125 - Third parties involved in tokenising reserve assets—The proposed third-party requirement is a sound starting point, but tokenisation of reserve assets creates a distinctive dependency that warrants explicit treatment when the tokenisation layer is material to reserve eligibility, ownership or control, liquidity, transferability or redemption. A PPSI may hold a technically valid token while the associated legal claim, custody record, entitlement, transfer restriction or redemption right is not what the token representation appears to imply. The Board’s own proposal recognises that a PPSI may rely on a tokenisation firm to ensure that a circulating token confers specified legal rights to the associated asset.

Materiality should turn on whether the third party can affect reserve eligibility, legal entitlement, valuation, liquidity, availability for redemption, or the PPSI’s ability to evidence those states.

Supervisory expectation. For a material tokenisation dependency, the PPSI should be able to produce a concise control record showing (i) the regulated function affected; (ii) the authoritative record and responsible entity; (iii) the active technical representation and version; (iv) persons or keys able to change, pause or revoke that representation; (v) reconciliation frequency and exception thresholds; (vi) the documented fallback or hold state; and (vii) evidence from the most recent test. For an ancillary representation that cannot affect reserve eligibility, availability or redemption, a lighter inventory-and-change-control record may be sufficient.

For a material tokenised reserve position, the PPSI should be able to establish at least the following:

- the underlying reserve asset and the legally relevant claim or entitlement represented by the token;
- the authoritative record or institution for ownership, custody, entitlement or other legally relevant state;
- the token issuer, tokenisation provider, custodian and any separate administrator or transfer agent, including their respective responsibilities;
- the active token or smart-contract version, privileged change authorities, pause, freeze, burn and recovery functions;
- the process for detecting and reconciling an on-chain/off-chain state mismatch;
- the treatment of corrections, revocations, corporate actions, asset substitution, insolvency, provider failure and migration;
- the conditions under which the token remains eligible, liquid and operationally available for redemption purposes; and
- the audit evidence required to demonstrate the source state and the PPSI's reliance at a relevant point in time.

These expectations could remain principles-based. The objective is not to require a particular token standard, oracle or registry, but to prevent a PPSI from treating technical possession of a token as sufficient evidence of the reserve asset's legal and operational availability.

Divergent-state protocol—Where the technical representation and the legally or operationally authoritative state diverge, the PPSI should not infer legal effect from the ledger alone. For a material reserve position, procedures should identify the prevailing source for the relevant purpose, place the affected position into a defined exception state, prevent new reliance on the disputed representation where necessary, preserve evidence sufficient to reconstruct both states, escalate to the responsible custodian, registrar, tokenisation provider or legal function, and resume normal treatment only after documented reconciliation or another legally valid resolution. Where the dispute concerns title, control, insolvency or another issue that cannot be resolved operationally, the control should preserve assets and records while the applicable legal process determines the outcome.

Question 126 - Smart contracts, encryption and other technology—The Board should expressly recognise lifecycle risk where smart contracts or cryptographic control mechanisms perform a material function in issuance, transfer, redemption, custody, reserve management or mandatory compliance. A general requirement to manage technology risk is useful, but supervisory expectations would benefit from non-prescriptive examples of the minimum control attributes that should be observable for a critical smart contract. A purely advisory or non-binding tool should not automatically be subject to the same depth of lifecycle control as code that can mint, burn, freeze, transfer or otherwise alter a regulated state.

Those attributes should include code or service identification; version; deployment and upgrade authority; privileged keys and key-recovery controls; upstream data and oracle dependencies; testing and change-approval records; transaction-state semantics; pause, freeze, rollback or compensating-control logic where legally and operationally available; incident and vulnerability handling; and evidence required to reconstruct the state that supported a regulated action. Encryption requirements should similarly be outcomes-based and should address key governance, rotation, recovery, access control, cryptographic agility and the risk that a cryptographic mechanism remains technically valid after the underlying authority, credential or entitlement has changed.

Question 127 - Transfers across blockchains to satisfy redemption—Principle. The Board should use principles-based requirements rather than prescribe a single locking, minting or burning model. The regulated outcome should be that cross-chain execution does not create uncertainty over supply, redemption liability, ownership or the status of the token being redeemed.

Supervisory expectation. Where a bridge is material to redemption, the PPSI should document the canonical issuance state, the events that change or extinguish liability on each network, responsible parties and privileged authorities, double-issuance/double-redemption controls, and a tested degraded-state response. That response may include circuit breakers or operational holds, suspension of reliance on the affected representation, an unaffected supported-network or direct issuer redemption path, heightened reconciliation, and evidence preservation. These controls should be consistent with 12 U.S.C. 5903(a)(6)(B): the PPSI need not control every external network, but it should retain enough control over issuance, redemption and supported access paths that a single unmanaged dependency cannot make compliance with a lawful order operationally impossible.

Materiality scaling. Enhanced controls should apply where the bridge or cross-chain mechanism is on the critical path to redemption, changes issuer liability, or is necessary for lawful-order execution. Optional distribution or routing functions that do not affect those outcomes may be subject to lighter controls, provided the PPSI can demonstrate a reliable alternative path.

Question 128 - Data privacy—Additional privacy requirements should be framed as privacy-preserving accountability. The objective should not be anonymity from the PPSI or competent authorities, but minimisation of unnecessary transmission, display and duplication of personal or commercially sensitive information across technical layers.

Subject to applicable U.S. law, the Board could recognise architectures in which full underlying information remains with the responsible institution or authoritative source while another participant receives only the role-specific information or evidence necessary for the regulated purpose. Controls should address purpose limitation, role-based access, encryption in transit and at rest, transaction binding, retention, audit logs, correction and lawful authority access. A reference, pseudonymous identifier or cryptographic proof should not be presumed non-personal merely because it does not display a customer name in clear text.

The rule should also preserve the distinction between underlying information and a derived compliance outcome. A binary or coded result can itself reveal sensitive information when associated with a customer, wallet or transaction. Access to adverse or investigative outcomes should therefore be limited to the minimum semantics and recipients necessary for the relevant function.

Privacy-preserving proofs—Where legally sufficient for the specific purpose, signed attestations and privacy-preserving cryptographic proofs, including zero-knowledge techniques, may reduce unnecessary disclosure between technical participants. They can demonstrate a narrowly defined fact or successful control without publishing underlying personal data on a public ledger. They should complement, not displace, the PPSI's access to information and records required for its own BSA/AML, sanctions, recordkeeping, investigation and lawful-order obligations. Proof semantics, issuer authority, expiry or revocation, transaction binding and auditability should therefore be governed explicitly.

Question 129 - Risks from blockchains on which payment stablecoins circulate—The proposed requirements should recognise that blockchain risk is heterogeneous and materiality-dependent. Relevant risks may include ledger unavailability, reorganisation or finality uncertainty; governance or protocol changes; smart-contract vulnerabilities; validator or

sequencer concentration; censorship or transaction-ordering risk; fee or congestion shocks; compromised privileged keys; chain splits; unreliable external data; and loss of access to information necessary to identify or service holders. The supervisory depth should depend on whether the network condition can impair issuance, redemption, reserve integrity, custody, lawful-order capability or mandatory compliance, rather than on the mere use of a particular blockchain architecture.

The PPSI should not be expected to control the underlying blockchain, but it should understand and document which blockchain characteristics are material to its regulated obligations and what operational response follows when those characteristics change. Supervisory expectations should focus on consequences: can the PPSI still determine supply, accept and process redemption, comply with lawful orders, perform BSA/AML and sanctions controls, maintain accurate books and records, and reconcile its liabilities? This consequence-based approach is more durable than a list tied to current blockchain designs.

Question 130 - Information-technology risks from tokenised reserve assets—Principle. The information-security program should expressly cover tokenised reserve assets when the technology is material to reserve eligibility, access, transferability, valuation, liquidation or timely redemption. The rule should remain technology-neutral: DLT use alone should not be treated as inherently higher or lower risk.

Supervisory expectation. For a material tokenisation layer, the PPSI should be able to demonstrate source-to-token reconciliation, the legally relevant ownership or entitlement record, active contract/version and privileged authorities, key and access controls, third-party and oracle/bridge dependencies, change and recovery procedures, and the ability to transfer or liquidate the reserve under stress. If the token state diverges from the authoritative record, reserve reliance should follow the documented prevailing-source and reconciliation rule.

Materiality scaling. Where tokenisation is only a representational or reporting layer and a conventional authoritative record plus an immediate operational fallback remain available, the control burden can be lighter. Enhanced controls are warranted where failure of the tokenisation layer could impair reserve availability, legal usability, liquidity, one-to-one backing or redemption.

Question 131 - Enterprise-wide risk management—DigitalTrade4.EU supports the proposed ability to use an enterprise-wide risk-management framework where it genuinely incorporates the PPSI's distinctive risks. This can reduce duplication and improve consolidated oversight. The Board should, however, expect the parent framework to identify stablecoin-specific dependencies rather than assume that conventional bank controls automatically cover them.

A parent framework should explicitly map minting and burning controls, private-key governance, chain and smart-contract dependencies, tokenised reserve assets, third-party digital-asset services, BSA/AML and sanctions interfaces, redemption continuity and any cross-chain mechanisms. The Board could assess adequacy by reviewing whether these dependencies are incorporated into risk appetite, incident management, change management, third-party oversight, testing, audit and business-continuity arrangements.

Illustrative enterprise-risk failure modes—The Board could test for two gaps that a conventional bank-level framework may otherwise miss. First, a parent framework may treat a cloud or software vendor as an ordinary ICT provider even though the vendor controls a privileged key or smart-contract upgrade path that can affect minting, burning or redemption. Second, a parent framework may treat reserve custody and stablecoin operations as separate risk domains even though a tokenisation platform or bridge creates a common dependency between reserve availability and redemption. The corrective expectation is not a separate parallel ERM

system, but explicit mapping of these stablecoin-specific dependencies into existing risk appetite, escalation, testing, audit and business-continuity processes.

5. Responses to Interoperability and Fraud Questions

Question 249 - Compatibility and interoperability standards—The Board and other primary Federal payment stablecoin regulators should distinguish technical connectivity from semantic, legal and operational interoperability. A standard can make two systems exchange data or tokens without ensuring that they agree on the meaning of an identifier, the legal claim represented by a token, the current status of a customer or entitlement, the applicable compliance state, or the event that constitutes completion or redemption.

Standards are most useful where they establish common functional expectations without mandating a single technology. DigitalTrade4.EU recommends that the regulators assess whether a minimum common interoperability profile is needed for material inter-PPSI and ecosystem interactions. The profile can be organised around five continuity outcomes: identity continuity (the responsible issuer, institution, account or wallet and authorised actor remain resolvable); claim continuity (the legal claim or form of value remains clear across representations); compliance continuity (required BSA/AML and sanctions information and evidence remain usable across regulated legs); audit continuity (transaction, source, version and status history remain reconstructable); and fallback continuity (participants know how to stop, reconcile, reroute or recover when systems disagree or a component fails).

- **Identity continuity:** stable issuer, institution, account/wallet and authority identifiers, with governed change semantics.
- **Claim continuity:** the form of value, legal claim, responsible obligor or servicing institution, and authoritative record remain identifiable across technical representations.
- **Compliance continuity:** required customer/payment information, screening evidence and relevant status remain available to the responsible regulated institution without unnecessary duplication.
- **Audit continuity:** transaction/message identifiers, provenance, versions, timestamps and lifecycle events remain traceable across transformations and technical rails.
- **Fallback semantics:** common meanings for hold, reject, retry, freeze, burn, redemption, correction, failed execution and reconciliation where systems disagree or become unavailable.

Implementation form— The profile need not create a new global database, ledger or token format. It can be implemented through existing message standards such as ISO 20022 where appropriate, governed APIs, verifiable credentials, signed attestations or comparable mechanisms. No single mechanism independently demonstrates compliance; the success criterion is preservation of regulated meaning and usable evidence across the end-to-end process.

Table 2. Minimum Interoperability Profile for material PPSI interactions.

Function	Minimum outcome	Illustrative supervisory evidence	Supervisory relevance
Identity continuity	Issuer, institution, account/wallet and authorised actor remain resolvable across technical steps.	Authoritative identifiers; change/revocation history; mapping between aliases, wallets and responsible institutions.	Reduces issuer, counterparty and authority impersonation risk.

Claim continuity	The form of value, legal claim, obligor/servicing institution and authoritative record remain clear across representations.	Legal/custody documentation; source-to-token mapping; conversion/bridge state; prevailing-source rule.	Prevents technical movement from obscuring the issuer liability or reserve claim.
Compliance continuity	Required BSA/AML and sanctions information and evidence remain available to the responsible regulated institution across regulated legs.	Transaction binding; source references; screening/decision record; bridge/conversion trace; exception handling.	Reduces blind transfers and preserves accountable compliance.
Audit continuity	Transaction, source, version, status and material lifecycle events remain reconstructable.	Stable identifiers; timestamps; version history; change approvals; retained exception and fallback evidence.	Supports examination, investigation, reconciliation and lawful-order response.
Fallback semantics	Participants have governed meanings and actions for hold, reject, retry, freeze, burn, correction, failed execution and reconciliation.	Runbook; circuit-breaker/hold criteria; authorised fallback; test results; restart/reconciliation approval.	Protects redemption and prevents inconsistent states from being treated as final or usable.

Question 250 - Interoperability, cross-chain bridges and BSA/AML/sanctions—Cross-chain bridges can reduce fragmentation but introduce additional trust, software, custody, governance and information dependencies. The principal regulatory concern is that moving a token between networks can separate the value-transfer event from the identity, compliance and audit information required by the responsible institution.

For BSA/AML and sanctions purposes, a PPSI should preserve the complete regulated transfer context across bridge or interoperability steps. This does not necessarily require every blockchain transaction to carry all customer information in clear text. It does require the responsible institution to be able to identify the relevant parties and accounts or wallets, the form of value transferred, the regulated intermediaries, the bridge or conversion steps forming part of the transaction, the source of required information, and the evidence showing what screening or other required checks were performed.²

U.S. compliance anchor— Proposed § 247.13(d) expressly ties the PPSI framework to applicable Bank Secrecy Act requirements and implementing regulations in 31 CFR Chapter X, together with specified GENIUS Act AML/CFT duties. The practical implication for interoperability is not to create a new federal data standard in this rule. It is to ensure that a bridge, wallet, analytics provider or other technical layer does not make required information, screening evidence or lawful-order capability unavailable to the regulated PPSI. Public-chain transparency and third-party analytics can support controls, but they should not displace the PPSI’s underlying legal obligations or accountability.¹

The Board should avoid treating public on-chain visibility or blockchain-analytics output as a substitute for underlying customer and payment information where law requires that information. Analytics may support risk detection, but a risk score or screening outcome is derived evidence. It should remain traceable to the relevant inputs, model or service version and accountable institutional decision.

Operationally, bridge controls should also address smart-contract compromise, key compromise, message forgery, replay, delayed finality, inconsistent states, chain reorganisation, insolvency or failure of the bridge operator, loss of compliance metadata and the possibility that a destination token no longer carries the same enforceable claim. Where a bridge is material, the PPSI should maintain a documented stop and fallback path and test both prospective continuity and retrospective reconstruction.

For material interoperability paths, the PPSI should also define a compliance-degraded state. If party information, sanctions status, authoritative identity evidence or another required control cannot be resolved within the applicable decision window, the transaction should be held, rejected or routed to a controlled review path rather than treated as cleared merely because the bridge or ledger leg is technically executable. This distinction between technical executability and regulated permissibility is especially important where a third-party bridge is outside the PPSI's direct control.

Question 251 - Fraudulent tokens and authenticity—The Board should support verifiable authenticity, but should avoid prescribing a single electronic-signature mechanism for all stablecoins. Fraud mitigation should allow a recipient, intermediary or wallet provider to determine whether a token representation is associated with the genuine issuer and an authorised issuance contract or equivalent mechanism, whether that representation is current, and whether it has been superseded or revoked.

A practical approach is to require PPSIs to publish or make securely resolvable authoritative issuer and token identifiers, including the active issuance contracts or equivalent technical representations on supported networks. The process should include change and revocation semantics so that a signature over an obsolete contract address does not continue to imply authenticity. Wallets and intermediaries should be able to validate this information through standardised, machine-readable means.

The Board should also consider ecosystem-level fraud patterns beyond counterfeit token contracts. Relevant examples include issuer impersonation through look-alike domains or support channels; wallet or bridge user-interface spoofing that redirects a user to an unauthorised contract or endpoint; fraudulent or replayed compliance attestations; misleading token symbols, logos or metadata; and unauthorised API or signing endpoints. These patterns can exploit a technically genuine network while deceiving the user about the issuer, destination, authority or compliance state. Authenticity should therefore be tied to the legal issuer and authorised technical representation, not merely to a ticker, logo, contract name or public-chain appearance.

Machine-resolvable change information should support automated warnings by wallets, exchanges and other regulated or supervised intermediaries. A PPSI could publish, through an authoritative channel, the currently supported domains and API endpoints used for issuer communications, active and superseded token or contract identifiers, supported networks, relevant signing keys or verification methods, and effective-time or revocation information. This would help counterparties distinguish an authorised representation from issuer impersonation, look-alike domains, spoofed wallet or bridge interfaces, fabricated compliance attestations and stale technical endpoints. The final rule should remain outcomes-based and should not prescribe a single public-key, domain or registry technology.

Proportionate authenticity controls— A PPSI should maintain authoritative, machine-resolvable information on supported networks, active issuance contracts or equivalent identifiers, and superseded or revoked representations. Wallets, custodians and intermediaries can then validate issuer and representation authenticity. The Board need not prescribe one

signature scheme; it can require an outcome in which authenticity and revocation are reliably discoverable and auditable.

Operational response to suspected ecosystem fraud—Where the PPSI cannot resolve the authenticity or current authority of a material token contract, bridge endpoint, issuer domain/API, signing key or compliance attestation, it should suspend reliance on the affected representation or endpoint for the regulated function it controls, preserve the relevant technical and audit evidence, route new activity to a documented lawful fallback or hold state, and reconcile the affected transactions before normal reliance resumes. Escalation should be proportionate to the consequence: an informational display anomaly need not trigger the same response as a compromised endpoint used for minting, burning, redemption, customer instruction or compliance gating. The final rule need not require the PPSI to control or halt a public network; it should require the PPSI to control its own reliance and regulated actions when authenticity cannot be established.

6. Implementation and Supervisory Assurance

Illustrative supervisory use case— Consider a PPSI that holds a portion of otherwise eligible short-term Treasury reserves through a third-party tokenisation platform, uses a bridge to make the stablecoin available on a second network, and uses an external blockchain-analytics service in its BSA/AML and sanctions workflow. During an examination, the Board need not inspect every line of code or receive every underlying customer record. It could request the PPSI's material-dependency map; the legal and custody documentation for the tokenised reserve claim; active contract and privileged-authority information; the bridge's supply and redemption-state controls; the analytics service's source, version and decision-use record; recent change notices; and results of fallback or mismatch tests.

What the examiner can test— A sample-based review could trace one reserve position and one regulated transfer from authoritative source to technical representation to PPSI decision, then introduce a controlled exception: for example, a stale tokenised-reserve status, a bridge leg that does not complete, or an analytics output that becomes unavailable. The examination objective would be to determine whether the PPSI can detect the condition, identify the responsible source and provider, stop or reroute safely, preserve required compliance controls, restore a usable state and reconstruct the decision. This converts dependency-lineage concepts into observable supervisory evidence rather than a new reporting regime.

Illustrative examination trace—A practical sample test could proceed as follows: (1) select one reserve position represented by a tokenised short-term Treasury asset; (2) obtain the custodian or other legally relevant source record showing the underlying asset, ownership or entitlement and effective time; (3) reconcile that source state to the tokenisation platform's issuance record and the active smart-contract version; (4) identify the privileged authorities, keys and third parties able to mint, burn, pause, upgrade or alter the representation; (5) trace one stablecoin issuance or redemption decision that relied on that reserve position, including any bridge, oracle or analytics output; (6) verify that the PPSI retained the source references, versions, timestamps and accountable approvals needed to reconstruct the decision; and (7) inject a controlled mismatch—such as a delayed source update, revoked attestation or unavailable bridge—and confirm that the documented hold, escalation, fallback and reconciliation path works as designed. The objective is not for the Board to re-perform every transaction, but to test whether the PPSI can prove the integrity and continuity of a material dependency chain.

Non-prescriptive supervisory examples—(1) Tokenised reserve: where a conventional custodian or securities record is authoritative and a third-party DLT token is representational,

an examiner could verify that the PPSI reconciles the authoritative source to the token state and suspends reserve reliance if the two diverge beyond a defined threshold. (2) Cross-chain redemption: an examiner could simulate failure after value is locked or burned on one network but before the corresponding step completes on another, and verify that supply, customer entitlement and redemption obligations remain determinable and that the PPSI enters a governed hold/fallback state. (3) Privacy-preserving compliance: where a signed attestation or cryptographic proof is used to minimise data sharing, an examiner could verify the attester's authority, proof semantics, expiry/revocation, transaction binding, the PPSI's access to underlying records where legally required, and the documented action when the proof cannot be validated.

Proportionality—The recommended controls should apply according to functional criticality. A third-party analytics service that provides non-binding supplementary information should not necessarily face the same evidentiary and continuity expectations as a service whose output determines whether stablecoins can be minted, burned, redeemed or supported by eligible reserve assets. The Board can preserve proportionality by focusing on the consequence of output failure or unusability and the availability of lawful fallback.

Testing—Testing should include more than a complete outage. For material dependencies, a PPSI should periodically test a reachable service that returns stale, revoked, inconsistent or context-mismatched information; loss of source-status access; failed cross-chain completion; privileged smart-contract change; and tokenised-reserve reconciliation failure. The metric should be time to restore a legally and operationally usable state, not only time to restore network connectivity.

Change management—Material changes to a smart contract, tokenisation platform, bridge, blockchain, source system, compliance service or access model should trigger an impact assessment and proportionate re-testing where the change could affect issuance, reserve integrity, redemption, custody, BSA/AML or sanctions performance. A PPSI should retain sufficient version and audit information to explain which state and controls applied to prior regulated actions.

Third-party portability and exit—Contractual exit rights are useful only if the PPSI can continue the regulated function or safely suspend it while preserving evidence. For material services, portability should include the source references, current-status semantics, versions, transaction binding and historical audit evidence needed to migrate or reconstruct the process. Data export alone may be insufficient if the replacement provider cannot lawfully query the authoritative source or interpret the historical state.

Supervisory transparency—The Board should be able to understand material dependencies without requiring routine access to all underlying personal, commercial or cryptographic secrets. A compact dependency and evidence-lineage record can provide the identity of the source and provider, function, version, status semantics, change authorities, failure modes, fallback and testing evidence while leaving sensitive underlying records within their competent systems where appropriate.

Assurance and certification—Independent testing, audit reports, certification or conformity assessment can provide useful evidence about smart-contract controls, bridge security, tokenisation platforms, cryptographic modules or other third-party services. The Board could recognise such evidence as one input to due diligence and ongoing monitoring, particularly where a common test profile improves comparability. Assurance should remain scoped to the function actually tested and should disclose relevant versions and limitations. It should not be treated as regulatory authorisation, proof of the legal effect of a tokenised claim, or a substitute

for the PPSI's responsibility for reserve integrity, redemption, BSA/AML, sanctions or other applicable obligations.

Table 3. Suggested supervisory mapping for material digital dependencies.

Dependency	Minimum questions for the PPSI	Primary risk outcome
Tokenised reserve asset	What legal claim is represented? Which source or record prevails? Who can change the token or underlying state? How is divergence detected and reconciled?	Reserve eligibility, liquidity and one-to-one backing
Smart contract	Which version is active? Who can upgrade, pause or administer it? What are the upstream dependencies and fallback conditions?	Unauthorised issuance, transfer or loss of control
Cross-chain bridge	What event changes liability on each chain? How are linked legs reconciled? What happens on failure, reorganisation or compromise?	Supply integrity, redemption and settlement continuity
Compliance / analytics service	What source data and model/service version produced the result? What is the permitted reliance? What happens if the result is stale or unavailable?	BSA/AML, sanctions and accountable decision-making
Identity / credential service	Who is the authoritative issuer? Is the authority current? Is the credential bound to the correct party and transaction?	Customer and authority attribution
Custody / key service	Who controls keys? How are segregation, recovery, rotation and emergency actions governed?	Asset control and operational continuity
Blockchain / network dependency	Which network conditions are material to issuance or redemption? What governance, finality, congestion, reorganisation or halt scenarios are monitored? What alternate path exists?	Issuance/redemption continuity and lawful-order capability
Oracle / external data feed	Which source is authoritative? What version/status semantics apply? How are stale, corrected or conflicting states detected? What is the stop/fallback rule?	Reserve, compliance or transaction-state integrity
Token authenticity / issuer metadata	Which representations are authorised? How are active, superseded and revoked identifiers published and verified?	Fraud prevention and representation authenticity
Issuer communications / API authenticity	Which domains, API endpoints, signing keys or verification methods are authoritative? How are changes, compromise and revocation published?	Issuer impersonation, spoofed interfaces and stale endpoint risk

7. Suggested Non-Prescriptive Regulatory Language

The following examples are offered as preamble or supervisory-guidance language rather than as mandatory technical specifications. They are intended to translate the principles above into observable supervisory outcomes while preserving the Board's technology-neutral approach.

Tokenised reserve assets—“Where a Board-supervised PPSI relies on a tokenised representation of a reserve asset for a material reserve-management or redemption function, technical possession or control of the token should not, by itself, be treated as sufficient evidence of reserve eligibility, legal entitlement, availability or liquidity. The PPSI should maintain controls reasonably designed to identify the legally or operationally authoritative state, reconcile material differences, and enter a documented hold or fallback state when the relevant states cannot be reconciled.”

Interoperability—“For purposes of assessing compatibility and interoperability under 12 U.S.C. 5912, the Board could consider whether a material interoperability arrangement preserves continuity of identity, legal claim or form of value, required compliance information, auditability and fallback semantics across participating systems. Technical connectivity alone does not establish that these regulated meanings remain usable.”

Lawful-order and critical-dependency capability—“A Board-supervised PPSI need not control an external blockchain or interoperability service. Where an external technical dependency is material to issuance, redemption, custody or compliance, however, the PPSI should maintain a feasible means to comply with applicable lawful orders and to suspend, reroute or otherwise control its own regulated activity when the dependency is unavailable, compromised or no longer produces a usable state.”

8. Proposed Consolidated Principle

DigitalTrade4.EU suggests that the Board consider a consolidated implementation principle along the following lines:

Where a Board-supervised PPSI relies on a tokenised asset, distributed ledger, smart contract, bridge, identity service, analytics service or other third-party digital infrastructure for a material regulated function, the PPSI should maintain controls proportionate to the function’s criticality that enable it to identify the authoritative source or legally relevant state, the responsible entities, the active technical representation and version, the permitted reliance, material changes and corrections, transaction or context binding, failure and fallback conditions, and the audit evidence necessary to reconstruct the regulated action. Technical verification or interoperability should not, by itself, determine legal effect or displace the PPSI’s responsibility under applicable law.

This formulation is intentionally technology-neutral. It does not mandate a registry, oracle, credential framework, blockchain type or data architecture. It focuses instead on what a supervised institution should be able to know and demonstrate when a digital dependency becomes material to a regulated function.

9. Conclusion

R-1899 provides an appropriate opportunity to establish a durable supervisory framework for payment stablecoins without freezing current technical architecture into regulation. The proposal already recognises that PPSIs may rely on smart contracts, private-key services, blockchain monitoring and tokenisation providers and that interoperability may create both opportunities and risks. DigitalTrade4.EU recommends building on that foundation through principles-based requirements for dependency lineage, current-state validity, tokenised-reserve legal and operational mapping, cross-chain lifecycle controls, privacy-preserving accountability and BSA/AML and sanctions information continuity.

The central policy objective should be controlled interoperability rather than connectivity for its own sake. A PPSI should be free to use different technical systems where it can still demonstrate what legal claim or regulated state is relevant, which source is authoritative, how the state was verified, which institution remains accountable, how a failure or correction is handled and how the decision can later be reconstructed. This approach can support innovation while preserving the one-to-one reserve, redemption, compliance and safety-and-soundness outcomes that the GENIUS Act and the Board’s proposed rule seek to protect.

Notes and References

1. Board of Governors of the Federal Reserve System. Implementing the Federal Reserve Board’s Responsibilities under the GENIUS Act. Docket No. R-1899; RIN 7100-AH29. Notice of Proposed Rulemaking, September 2026.
2. DigitalTrade4.EU. Payment Transparency, Interoperability and Trusted Digital Compliance under FATF Recommendation 16. Public consultation submission, August 2026.
3. DigitalTrade4.EU. Proposal and Recommendations for the European Commission’s Review of the Markets in Crypto-Assets Regulation (MiCA): European Digital Financial Trust Framework. Version 7.0, September 2026.
4. DigitalTrade4.EU. Response to CPMI-IOSCO Discussion Paper: FMIs’ Reliance on Third-Party Service Providers: Challenges and Risks. Version 7, 23 September 2026.
5. Vedler, R. Verified Trade Events and Trade-Finance Interoperability: Working Capital and End-to-End Frictions in Global Value Chains. DigitalTrade4.EU, September 2026.
6. Board of Governors of the Federal Reserve System. Federal Reserve Board requests public comment on two proposals related to establishing a regulatory framework for Board-supervised payment stablecoin issuers under the GENIUS Act. Press release, 24 September 2026.
7. United States. Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), Pub. L. No. 119-27 (2025), codified at 12 U.S.C. 5901 et seq.; see particularly 12 U.S.C. 5903(a)(6)(B) and 5912 as cited in the Board’s proposed rule.

Appendix A. Selected R-1899 Question Map

Table A1. Questions addressed in this Version 5 submission.

Question	Subject	DigitalTrade4.EU response focus
124	Scope of risk management	Information-state risk, function-level dependency mapping
125	Third parties tokenising reserve assets	Legal claim, authoritative record, lifecycle, reconciliation and fallback
126	Smart contracts, encryption and technology	Lifecycle governance, privileged authority, cryptographic agility and auditability
127	Cross-chain transfers for redemption	Canonical state, supply integrity, linked-leg failure and safe fallback
128	Data privacy	Privacy-preserving accountability, minimisation and role-based access
129	Blockchain risks	Consequence-based assessment of ledger, governance, finality and operational risks
130	Tokenised reserve asset IT risks	Source-to-token integrity, legal usability, recovery and liquidity under stress
131	Enterprise-wide risk management	Stablecoin-specific dependencies within consolidated controls
249	Interoperability standards	Functional and semantic interoperability rather than one mandated technology
250	Cross-chain, BSA/AML and sanctions	Information continuity, accountable compliance and bridge controls
251	Fraudulent tokens	Machine-verifiable issuer and token authenticity with change/revocation semantics

Status. Version 5 is a working consultation draft prepared from the Federal Reserve Board R-1899 proposal and the referenced DigitalTrade4.EU materials. Question numbers and proposed-section references correspond to the September 2026 R-1899 notice used for this draft and should be checked against the Federal Register publication before filing. The suggested regulatory language is non-prescriptive drafting for consideration and does not purport to reproduce or replace the Board's proposed rule text.