ERC-8319: Regulatory Compliance Protocol

Standards Track / ERC

Field	Value
eip	8319
title	Regulatory Compliance Protocol
description	A protocol defining the legal effect of regulatory enforcement actions on tokenized assets and the requirements they address
author	Jinwook Kim (@jay-oraclizer), Rob Viglione <rob@horizenlabs.io>, Dan Spuller <dan@theblockchainassociation.org>
discussions-to	https://ethereum-magicians.org/t/erc-8319-regulatory-compliance-protocol/28917
status	Draft
type	Standards Track
category	ERC
created	2026-07-03

1 Abstract

This EIP defines the Regulatory Compliance Protocol (RCP), a shared definitional layer that assigns explicit legal effect to regulatory enforcement actions on tokenized assets, expressed as a controlled vocabulary. It defines a closed set of six regulatory actions (FREEZE, SEIZE, CONFISCATE, LIQUIDATE, RESTRICT, RECOVER), each with explicit legal semantics of reversibility and ownership effect, and organizes 31 compliance requirements, compiled from the published guidance of 15 financial regulatory authorities, under five principles that together map the regulatory surface a tokenized asset must address. The need for such a layer is observable today: deployed security token standards expose legally distinct enforcement actions through a single undifferentiated control function, so that on-chain a reversible freeze and an irreversible confiscation cannot be distinguished, and no shared, citable definition of these actions exists for standards or tooling to reference. RCP supplies that definitional layer. RCP standardizes the meaning of these actions rather than the functions through which a contract exposes them: it defines no on-chain interface and introduces no code dependency. Its normative requirements apply only to a standard that claims conformance to the vocabulary, so any standard may reference it voluntarily and non-disruptively, or not at all.

---

2 Motivation

2.1 The Missing Vocabulary (Observable Today)

Existing Ethereum security token standards expose legally distinct enforcement actions through a single, overloaded control mechanism. ERC-3643 exposes an operator-driven forced transfer for any privileged movement of tokens, and earlier security token standards similarly route all privileged movement through a single `controllerTransfer` function. A regulator-mandated freeze (temporary, reversible, ownership unchanged) and a court-ordered confiscation (permanent, irreversible, ownership transferred) are, at the contract level, the same call; an on-chain observer (an auditor reconstructing events, an indexer, a counterparty assessing an asset's standing) cannot

determine from the call itself whether an action is reversible. This is observable in deployed code today. The issue is not that any individual standard is defective; it is that, across standards, the legal effect of an action is either absent or undefined. Minimal enforcement primitives carry no legal effect by design, and the specifications say so plainly: one widely deployed security token standard defines its single `controllerTransfer` for three legally divergent purposes at once, to *"reverse fraudulent transactions, resolve lost private keys and responding to a court order,"* while placing the data that would distinguish them *"outside the scope of this standard"*; and ERC-7943 selects the neutral name `forcedTransfer` precisely because names such as confiscation or recovery *"describe specific motivations"* that the primitive deliberately does not carry. Richer standards do expose named operations (ERC-3643's freeze, forced transfer, and recovery), but these are standard-specific function names rather than a shared taxonomy, and none of them defines the property that matters most: whether the action can be undone, and what becomes of ownership. That property is therefore expressed nowhere on-chain, and defined nowhere that a standard, an auditor, or a regulator could cite.

2.2 What RCP Provides

RCP fills this gap at the definitional layer. It defines a small, closed vocabulary of regulatory actions with explicit legal semantics, so that the distinction between them can be named, referenced, and described consistently. RCP is reference material, not an interface: it specifies what a confiscation or a freeze means (its reversibility and its effect on ownership), not how a contract should implement one. A standard or tool that adopts this vocabulary can map its own operations onto these shared terms, supplying the defined legal effect that a neutral primitive omits and that a standard-specific name leaves ambiguous, so that a confiscation is recorded as a confiscation rather than as an indistinguishable transfer. How those actions are exposed on-chain is left entirely to the Standards Track standards that choose to implement them.

2.3 Why a Shared Vocabulary, and Why Here

Naming is a coordination problem. Regulatory semantics also sit outside the working knowledge of most protocol engineers, and a standard author today has no neutral, citable reference inside the Ethereum process to point to for the legal effect of an enforcement action. If each standard invents its own terms for these actions (or, as today, either omits the distinction entirely or buries it in standard-specific names), then descriptions of compliance behavior are not comparable across standards, and a future Standards Track standard cannot reference a settled definition of, for example, an irreversible confiscation. A controlled vocabulary resolves this only if it has a single, stable, permanently citable home that other standards can reference by identifier and that is maintained under the same process and license as the standards that consume it. The EIP repository is that home; an external paper or a mutable web page is not. RCP is therefore offered here as an application-level convention in the sense of EIP-1: it standardizes a shared vocabulary and the legal effect each term carries, defines no interface, and constrains only those standards that choose to describe their behavior in its terms.

2.4 A Secondary Benefit: Cross-Standard Description

Beyond the present defect, a shared action vocabulary also makes it possible to describe and compare the compliance coverage of different standards consistently, including across chains and jurisdictions. RCP does not itself provide any cross-chain mechanism; portability of compliance state is left entirely to future Standards Track standards. RCP supplies only the common terms such work would build on, and it takes no position on whether or when such markets develop; it only ensures that if standards later address them, the terms are already settled. This benefit is real but secondary; the primary justification is the defect observable today, described above.

2.5 Gaps in Existing Standards

The Ethereum ecosystem has produced security token standards including ERC-3643 and the 1400 family. While these represent important progress, they address only portions of regulatory requirements without a unified conceptual framework. The specific defect this EIP addresses (enforcement actions exposed without their legal effect) is detailed above; the gaps below are the broader, mostly non-overlapping ones that motivate a shared reference base.

- No standardized regulatory action taxonomy: legal effects such as reversibility and ownership change are not named consistently across standards.
- No token expiration mechanism, though this is essential for instruments such as bonds and derivatives.
- No unified identity framework balancing privacy with regulatory oversight; ERC-3643 couples identity management to specific implementations.
- No shared basis for describing compliance coverage or portability of compliance state across chains and jurisdictions; this is left entirely to future Standards Track work, and RCP supplies only the common terms such work would build on.

Structural limitations also persist: the 1400 family is fragmented across multiple draft substandards and has not advanced to a finalized standard, and ERC-3643 is designed for single-chain, single-jurisdiction deployment with limited support for diverse asset classes.

2.6 Regulatory Requirements Are Already Stated

This protocol does not propose new interpretations of regulatory requirements. It systematically compiles what regulators have explicitly stated regarding distributed ledger technology and tokenized financial instruments. Through review of guidance documents from 15 regulatory authorities, we identified 31 requirements that these authorities have explicitly stated for DLT-based financial systems:

The World Bank states that DLT systems in financial contexts must comply with *"know-your-customer (KYC) and customer due diligence (CDD) requirements of anti-money laundering/ combatting the financing of terrorism (AML/CFT) regulations."* [1]

FINMA (Article 44(3)) requires that financial intermediaries *"ascertain and document the contracting party's authorisation provisions relating to the body corporate concerned and verify the identity of the individuals acting on behalf of a body corporate in establishing the business relationship."* [2]

HKMA identifies that *"Digital identity (D-ID) management has been identified as a possible means to streamline KYC processes, enabling multiple banks to rely on the same shared, secure, and auditable source of digitalised customer information."* [3]

FATF Virtual Asset Guidance states that *"VASPs and other obliged entities engaging in or providing VA activities, products, and services should have the ability to flag for further analysis any unusual or suspicious movement of funds or transactions, including those involving VA, or other activities indicative of potential involvement in illegal activities."* [4]

BIS-IOSCO establishes that *"An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time."* [5]

These represent explicit, published regulatory positions. The requirements themselves are sourced from the authorities; RCP's contribution is to select, organize, and classify them into a shared

vocabulary, and to assign each to a principle and, where applicable, to a class of regulatory action.

---

3 Specification

The substantive content of this EIP is a framework in two parts: a closed taxonomy of six regulatory actions (defined in the Regulatory Action Taxonomy below), each with explicit legal semantics of reversibility and ownership effect, which is the normative anchor; together with 31 compliance requirements, compiled from published regulatory guidance and organized under five principles, which is the descriptive reference base. The taxonomy carries the conformance meaning; the requirements record what the cited authorities have stated. RCP defines no on-chain interface; concrete interfaces are left to the standards that implement these actions. The normative requirements of this specification are conditional, and apply only to a standard, implementation, or tool that claims conformance to the RCP action vocabulary. Such a claimant MUST represent each distinct RCP action it supports as a distinct, separately observable operation, and MUST NOT apply an RCP action name to an operation whose reversibility or effect on ownership differs from the definition given in the Regulatory Action Taxonomy below. A standard that makes no such claim incurs no obligation under this specification, and adoption remains entirely at the discretion of each standard or tool.

The key words "MUST" and "MUST NOT" in this document are to be interpreted as described in RFC 2119 and RFC 8174.

3.1 Scope and Non-Exhaustiveness

This compilation is bounded to DLT-specific and tokenized-asset guidance published by the 15 authorities listed below, as of the dates of the cited documents. It is deliberately not exhaustive. Several well-established obligations are intentionally outside the 31 requirements because they are predominantly operational, off-chain, or jurisdiction-specific, and are better addressed by implementations or by future Standards Track work. These include, among others: transmission of originator and beneficiary information on transfers (the FATF Travel Rule, Recommendation 16); filing of suspicious activity or transaction reports to a competent authority, as distinct from on-platform monitoring; screening against official sanctions lists, as distinct from discretionary blacklists; segregation of client assets from proprietary assets; suitability and appropriateness assessment; and minimum recordkeeping retention periods. Jurisdictional coverage is likewise non-exhaustive; regimes not yet incorporated include, among others, the Japan FSA, the Republic of Korea FSC, and the UAE VARA. Contributions extending this coverage are welcome through the discussion thread.

3.2 Regulatory Authorities Reviewed

This protocol incorporates requirements from the following 15 authorities. Abbreviations are used throughout this document. The set mixes international standard-setters (for example, BIS, IOSCO, FSB, FATF) with national or regional regulators; both are sources of the requirements compiled here.

Abbreviation	Full Name
WB	World Bank
ISDA	International Swaps and Derivatives Association
IOSCO	International Organization of Securities Commissions

Abbreviation	Full Name
IMF	International Monetary Fund
FSB	Financial Stability Board
FATF	Financial Action Task Force
BIS	Bank for International Settlements
SFC	Securities and Futures Commission, Hong Kong
HKMA	Hong Kong Monetary Authority
EU	European Union Regulatory Framework
ESMA	European Securities and Markets Authority
FCA	Financial Conduct Authority, UK
MAS	Monetary Authority of Singapore
FINMA	Swiss Financial Market Supervisory Authority
FINRA	Financial Industry Regulatory Authority, US

This protocol also includes technical references from industry standards bodies (for example, the InterWork Alliance Token Taxonomy Framework; the InterWork Alliance is now an initiative of the Global Blockchain Business Council), which are classified separately as industry standards rather than regulatory authorities.

3.3 The Five Principles

The 31 requirements below are compiled directly from the published guidance of the 15 authorities listed, and organized under five principles as a reference base against which a standard can describe its own coverage. This organization is descriptive rather than normative; the taxonomy of regulatory actions is the part of this EIP that carries a conformance meaning, while the requirements record what the cited authorities have already stated. The five principles are derived from a functional analysis of those frameworks. Requirements are numbered 1 through 31 following the original RCP research numbering; the numbering is preserved for traceability and is not contiguous within each principle. For reference, principle membership by requirement number is: Traceability (1 through 6), Privacy (7, 17, 18), Enforceability (8 through 16), Finality (20 through 22), and Tokenizability (23 through 28, 30, 31). Requirements 19 (Code Security) and 29 (Gasless Support) are classified as non-normative implementation recommendations and are documented under Implementation Recommendations in the Rationale section rather than as core regulatory requirements. The complete regulatory reference base behind this survey, including the full set of source quotations compiled for every requirement, is maintained in the companion RCP reference paper [29]; the excerpts quoted under each requirement below are representative.

3.4 Principle 1: Traceability

Definition: The ability to identify, track, and audit all participants, assets, and transactions throughout their lifecycle.

Regulatory Basis: AML/CFT requirements, KYC obligations, transaction monitoring mandates.

(1) Customer Identity Verification. Regulators require verification of customer identity prior to establishing business relationships or conducting transactions.

> *"To be adopted in the financial system, DLT systems need to comply with know-your-customer (KYC) and customer due diligence (CDD) requirements of anti-money laundering/combatting the financing of terrorism (AML/CFT) regulations."* [1]

> *"Article 44(3): Where a contracting party is a body corporate or partnership, the financial intermediary must ascertain and document the contracting party's authorisation provisions relating to the body corporate concerned and verify the identity of the individuals acting on behalf of a body corporate or partnership in establishing the business relationship."* [2]

> *"9.5 A platform operator should take all reasonable steps to establish the true and full identity of each of its clients and, other than for institutional and qualifying corporate professional investors, ascertain the financial situation, investment experience and investment objectives of each of its clients."* [6]

(2) High-Risk and Suspicious Transaction Monitoring. Continuous monitoring of transactions to identify potential illicit activity is required.

> *"275. Risk-based ongoing monitoring means scrutinising transactions to determine whether the transactions are consistent with a VASP's (or other obliged entity's) information about the customer and business relationship's nature and purpose. Transactions which do not fit the expected behaviour from a customer profile or deviate from usual transaction patterns could be potentially suspicious."* [4]

> *"14.3.1 An FI shall implement real-time fraud monitoring systems to identify and block suspicious or fraudulent online transactions. 14.3.2 Processes should be in place to investigate suspicious transactions or payments and to ensure that issues are addressed appropriately and promptly."* [7]

> *"75. Many jurisdictions have specific requirements on AML/CFT and consumer protection. The former mainly includes customer due diligence, transaction monitoring and reporting of suspicious transactions."* [8]

(3) Detection of Changes to Customer Identity Information. Systems must detect and respond to changes in customer identity information.

> *"Customers may access the DLT network at any time to receive the hash entries of their own personal information and documents for the purpose of ascertaining whether or not their subsequent information and document updates have been verified by the accepting bank and the respective hash has been stored on the DLT network."* [3]

(4) Contract Version Tracking. An auditable, correctly ordered record of changes is needed for audit and compliance purposes, so that amendments can be tracked in sequence and each participant holds the same up-to-date record.

> *"149. ESMA considers that amendments under the transaction reporting regime rely on the fact that transaction report items are sequential (NEWT/CANC/NEWT) and therefore a DLT infrastructure not requesting a reporting exemption must have in place systems to ensure that the correct order is followed."* [11]

> *"32. Each party participating in the verification process has the same, up-to-date copy of the chain, or public ledger, which is a record of all transactions. Each party's copy of the ledger is updated each time a new block is discovered."* [10]

(5) Exploration of Transaction History by Asset Type. Regulatory oversight requires the ability to explore and audit transaction history by asset type.

> *"2.77 Ownership of a cryptoasset may change, for example, under certain complex yield models or contracts. In such cases firms should make clear and prominent disclosure to consumers of the change to the legal and beneficial ownership of the cryptoassets before the consumer enters into the relevant agreement."* [12]

> *"Recommendation 12: As is the case for traditional financial assets, regulators should set the expectation that CASPs should keep accurate and up-to-date customer asset records and accounts that readily establish the exact nature, amount, location and ownership status of the customer assets and the customer for whom the assets are held."* [13]

(6) External Audit Support. Independent external audit capability must be supported.

> *"11860. (b)(4) The term 'auditor's report' means a written report prepared by competent and independent external auditing personnel in accordance with standards of the American Institute of Certified Public Accountants."* [14]

> *"(41) . . . The competent authority for a DLT market infrastructure should be allowed to require an audit to ensure that the overall IT and cyber arrangements of the DLT market infrastructure are fit for purpose. The costs of the audit should be borne by the operator of the DLT market infrastructure."* [15]

> *"10.6. Accounting and auditing standards should ensure that fundamental information is available. There should be comprehensive and well-defined accounting principles of a high, internationally acceptable quality, and which provide accurate and relevant information on financial performance."* [16]

3.5 Principle 2: Privacy

Definition: Protection of sensitive information while maintaining necessary transparency for regulatory oversight.

Regulatory Basis: Data protection regulations, financial privacy requirements, need-to-know and least-privilege principles.

(7) Setting Role-Based Permissions. Access control based on roles and responsibilities must be implemented, so that information and sensitive functions are available on a need-to-know, least-privilege basis.

> *"9.1.1 The 'not alone', 'segregation of duties' and 'least privilege' principles should be applied when granting staff access rights to information assets so that no single person is in a position to have access rights for performing sensitive system functions. Access rights and system privileges should be granted according to the role and responsibilities of staff, contractors and service providers."* [7]

> *"3.4 The system should allow for distinguishable levels of permissions. Users should be able to designate the level of privacy for each transaction and to appropriately conceal identity, transaction patterns and contractual terms from unauthorized participants where necessary."* [3]

(17) Privacy of Personal Information. Personal information must be protected according to data protection principles.

> *"Apart from addressing the privacy of privileged information stored on DLT, it is important to consider the privacy of metadata stored on DLT. Apart from transactions being stored transparently, transacting public keys are anonymous but static, so that transactions and transaction parties can be easily tracked over time."* [3]

> *"Article 17 Right to erasure ('right to be forgotten'). The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her*

> *without undue delay, and the controller shall have the obligation to erase personal data without undue delay where one of the grounds applies."* [17]

(18) Privacy of Financial Transactions. Financial transaction data requires appropriate privacy protections.

> *"12300. (d)(1)(A) In all filings with the Director, a party shall redact all documents that contain an individual's social security number, taxpayer identification number or financial account number to include only the last four digits of any of these numbers."* [14]

> *"Recommendation 10: Regulators should require that CASPs have systems, policies and procedures in place for the handling of material non-public information, including where relevant information relating to whether a crypto-asset will be admitted to, or delisted from, trading on a platform, and information relating to customer orders, trade execution and personally identifiable information."* [13]

3.6 Principle 3: Enforceability

Definition: The ability for authorized parties to execute regulatory actions on tokenized assets.

Regulatory Basis: Asset freeze powers, seizure authorities, sanctions enforcement, court order execution.

This principle addresses the critical requirement that regulators must be able to intervene in tokenized asset markets when necessary. Current standards provide limited regulatory action capability through single functions (for example, a single `controllerTransfer` function), which is insufficient for distinguishing legally distinct actions.

(8) Asset Freeze. Regulators require the ability to temporarily halt transactions on specific assets.

> *"116. Recommendation 6. Countries should freeze without delay the funds or other assets, including VA, of designated persons or entities, and ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of designated persons or entities, in relation to targeted financial sanctions related to terrorism and TF."* [4]

> *"16. Countries should ensure that financial institutions take freezing action and prohibit conducting transactions with designated persons and entities, in the context of processing wire transfers, in accordance with the obligations set out in the relevant United Nations Security Council resolutions."* [9]

(9) Asset Recovery. Mechanisms for recovering assets in cases of fraud, theft, or court orders, including return to a rightful owner.

> *"Interpretive Note to Recommendation 40. B. 20. Countries should participate in and actively support multilateral networks to better facilitate prompt and constructive international cooperation in asset recovery."* [9]

(10) Trading Restrictions. Authority to impose restrictions on trading activity.

> *"2360. (b)(8) FINRA may from time to time impose restrictions on options trading or on the exercise of options contracts in one or more series of one or more options classes when FINRA deems the restriction necessary to maintain a fair and orderly*

> *market in the options contracts or the underlying securities, or as necessary for the public interest or the protection of investors."* [14]
>
> *"Article 17 Access to quotes. In order to limit the risk of exposure to multiple transactions from the same client, a systematic internaliser may limit in a non-discriminatory manner the number of transactions from the same client it undertakes to enter into under the published conditions."* [21]

(11) Transaction Limit. Setting limits on transaction amounts or frequency.

> *"Interpretive Note to Recommendation 10. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Interpretive Note to Recommendation 16. Countries may adopt a minimum threshold (no higher than USD/EUR 1,000) for cross-border wire transfers."* [9]
>
> *"9.7 Other than for institutional and qualifying corporate professional investors, a platform operator should set limits for each client, making reference to the client's financial situation (including the client's net worth) and personal circumstances, to ensure that the client's exposure to virtual assets is reasonable."* [6]

(12) Cancellation or Modification of Transactions. Authority to cancel or modify transactions under specific circumstances.

> *"Article 36 Essential requirements regarding smart contracts for executing data sharing agreements . . . (b) safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;"* [20]
>
> *"If certain events (such as a default or termination event) occur with respect to one party, the other party is not required to perform its payment obligations while that event is continuing. Accordingly payment obligations are 'suspended' for the duration of the event."* [19]

(13) Pausing of Trading. Authority to pause trading activity platform-wide or for specific assets.

> *"Article 9 Waivers for non-equity instruments. A competent authority supervising one or more trading venues on which a class of bond, structured finance product, emission allowance or derivative is traded may, where the liquidity of that class of financial instrument falls below the specified threshold, temporarily suspend the obligations referred to in Article 8."* [21]
>
> *"7.11 A platform operator should carry out ongoing monitoring for each virtual asset admitted to trading and consider whether to continue to allow trading. If the SFC decides to suspend or withdraw a virtual asset from trading, the platform operator should notify the clients as soon as practicable of the decision and the grounds for the decision."* [6]

(14) Suspension or Termination of Smart Contract (Kill Switch). Authority to suspend or terminate smart contract operation.

> *"Article 36 . . . (b) safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions; (c) data archiving and continuity, to ensure, in circumstances in which a smart contract must*

be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);" [20]

(15) Blacklist Management. Management of lists of prohibited addresses or entities.

"273. Where a VASP discovers VA addresses that it has decided against establishing or continuing a business relationship with, or transacting with, on the basis of ML/TF suspicions, VASPs should consider, subject to jurisdictional law, providing a list of 'blacklisted wallet addresses'. VASPs should screen wallet addresses of customers and counterparties against such available blacklisted wallet addresses as part of ongoing monitoring." [4]

"11540. (b) Where certain certificates submitted in settlement of foreign security contracts are on a blacklist, blocked list or similarly held in suspense and cannot be removed by the bona fide holder upon simple demand, such certificates are not good delivery and reclamation may be made thereon at any time without limitation." [14]

(16) Forced Liquidation. Authority for forced liquidation of positions under specific circumstances.

"4210. (g)(14)(A) A member must immediately liquidate all portfolio margin accounts that have a position in any of the affected products, or transfer the portfolio margin account to another broker-dealer that is qualified to carry portfolio margin accounts, if it is insolvent or unable to meet its obligations as they mature as defined in Section 101 of Title 11 of the United States Code." [14]

"Principle 13: Participant-default rules and procedures. A CCP should have rules and procedures that enable the prompt liquidation or transfer of a defaulting participant's proprietary and customer positions." [5]

"3.3.4. Some authorities may consider implementing broad-based restrictions, targeted or time-bound, to manage the risks of crypto-assets." [22]

3.7 Regulatory Action Taxonomy (Core Definitions)

These six actions and their legal semantics are the normative anchor of this EIP: the one part of RCP that carries a conformance meaning for a standard claiming to support these actions. They sharpen, but do not stand apart from, the broader framework of five principles and 31 requirements in which they sit. The 31 requirements are drawn directly from the cited authorities; their organization into five principles, and this six-action taxonomy with its reversibility and ownership-effect attributes, are RCP's own synthesis, derived by functional and legal analysis of those regulatory sources rather than transcribed from any single authority. No cited regulator publishes a closed list of enforcement actions with these legal-effect attributes; RCP proposes the classification precisely because that shared, citable distinction does not yet exist, and offers it as reference material open to correction. Current standards provide limited regulatory action capability; regulatory actions have distinct legal meanings requiring differentiation:

Action	Description	Reversibility	Ownership	Finality
FREEZE	Temporary transaction halt	Reversible	Retained	Provisional
SEIZE	Custody transfer to authority	Conditional	Retained	Interim custodial
CONFISCATE	Permanent ownership transfer	Irreversible	Transferred	Final

Action	Description	Reversibility	Ownership	Finality
LIQUIDATE	Forced conversion for debt	Irreversible	Terminated	Final
RESTRICT	Conditional trading limitations	Configurable	Retained	Conditional
RECOVER	Return to rightful owner	One-time	Restored	Restorative

Each action names the legal effect that its on-chain mechanism leaves unstated: FREEZE is a temporary, ownership-preserving hold, typically under a sanction or an injunction; SEIZE is a custodial transfer to an authority pending adjudication, with title retained; CONFISCATE is the permanent, irreversible extinguishment of the holder's title through forfeiture; LIQUIDATE is an irreversible forced sale to satisfy a debt or default; RESTRICT is a configurable, ownership-preserving limit on transferability; and RECOVER returns an asset to its rightful owner after loss, theft, or error. It is these effects, not the calling convention, that a single overloaded transfer function cannot distinguish.

The Finality column records a recognized gradation among the deprivation actions: in the FATF framework and in many jurisdictions, a freeze is a provisional restraint that only prohibits movement (no control taken) pending a later determination, a seizure additionally takes the asset into the custody or control of an authority on an interim basis, and a confiscation (which includes forfeiture) is the permanent deprivation of the holder's title, typically the outcome of a final court or authority decision. This yields a partial ordering along finality over the deprivation actions (FREEZE is less final than SEIZE, which is less final than CONFISCATE and LIQUIDATE), mirrored on-chain by the progression from a reversible, ownership-preserving hold to an irreversible transfer or termination of ownership. RESTRICT and RECOVER sit outside this ladder: RESTRICT is a conditional, ownership-preserving limit, and RECOVER is restorative rather than depriving. RCP records this gradation as it appears in the cited legal frameworks; it does not assert a total severity ranking, and the procedural thresholds for each step (for example, civil as opposed to criminal forfeiture) remain a matter of the applicable jurisdiction and its legal process.

A standard that claims to support these distinct regulatory actions represents them as distinct, separately observable operations, because the actions carry different legal implications and procedural requirements. A single `controllerTransfer` function cannot adequately represent these distinct regulatory mechanisms.

3.8 Principle 4: Finality

Definition: Assurance that transactions and ownership records are legally conclusive under defined conditions.

Regulatory Basis: Settlement finality requirements, legal documentation standards, immutability expectations.

(20) Immutability of the Ledger. The integrity and immutability of the distributed ledger must be maintained.

> *"A blockchain is immutable; once a transaction has been recorded it cannot be deleted, together with the multiple copies, this means the integrity of the ledger can be easily proven."* [3]

> *"Data Integrity: data stored on a ledger has a high level of integrity, requiring consensus among participants to alter any data block (depending on the specific rules of the distributed ledger)."* [11]

(21) Finality of Transactions and Payments. Transactions must achieve legal finality at a defined point.

> *"Principle 8: Settlement finality. An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time."* [5]

> *"A payment is final when it becomes both irrevocable and unconditional. The precise moment at which this occurs depends generally both on the underlying legal regime and on the rules of the payment system itself."* [5]

(22) Attaching Legal Documents. Legal documents must be attachable and verifiable.

> *"11540. (a) Where law, regulations, judgment, directive, or order of any government, governmental agency or agent, or official having jurisdiction, require a license, clearance certificate, affidavit of ownership or similar document to be obtained in connection with the acquisition, disposition, transfer, or redemption of securities or other transactions, such securities shall not be good delivery unless accompanied by such required documents."* [14]

> *"It will also be important for parties to agree on mechanisms, within or outside the smart derivatives contract, for verifying or validating accuracy of data inputs, as well as for determining how inaccurate data entries should be corrected and how responsibility for errors should be allocated."* [23]

3.9 Principle 5: Tokenizability

Definition: The ability to represent real-world assets as tokens while preserving their legal, economic, and regulatory characteristics throughout their lifecycle.

Regulatory Basis: Securities regulations, asset classification requirements, lifecycle management.

This principle addresses the fundamental requirement that tokenized assets must faithfully represent the characteristics of the underlying real-world assets, including temporal properties (expiration), classificatory properties, and restrictive properties (transfer limitations).

(23) Token Expiration Time. Tokens representing time-bound assets must support expiration mechanisms.

> *"2360. (a)(14) The term 'expiration date' in respect of an option contract issued by The Options Clearing Corporation means the date and time fixed for the expiration of such option contract pursuant to the rules of The Options Clearing Corporation."* [14]

This requirement addresses a fundamental gap in current standards: tokens representing bonds, options, and other time-bound instruments cannot exist indefinitely. A 10-year bond maturing in 2035 requires a mechanism for principal repayment and token retirement at maturity.

(24) Token Transfer Restrictions. Tokens must support configurable transfer restrictions based on regulatory requirements.

> *"109. A crypto-asset can be designed in a way that it does not allow for any transfer in capital markets. Some restrictions may be placed on negotiability by not allowing holders to negotiate and/or transfer crypto-assets to a person other than the issuer. In respect of any restrictions on the transfer of financial instruments, these need to be considered on a case-by-case basis, as the nature and impact of the restriction could be sufficient to render the instrument non-tradable, hence falling outside the definitional scope of 'transferable security'."* [24]

(25) Issuance of Tokenized Cash. Standards for representing cash or cash-equivalent instruments as tokens.

> *"5.1 (v) Tokenization is the process of digitally representing an asset, or the ownership of an asset. A token represents an asset, or the ownership of an asset. Such an asset can be a currency, commodity, security, or real estate."* [25]

(26) Issuance of Tokenized Securities. Standards for representing securities as tokens.

> *"In its Fintech Report, IOSCO noted that tokenization is the process of digitally representing an asset, or the ownership of an asset. A token represents an asset, or the ownership of an asset. Such an asset can be a currency, commodity, security, or real estate."* [26]

(27) Decimal Unit Control. Control over minimum trading units and decimal precision, including restrictions on subdividing a token below whole units.

> *"A restriction that there can only be 1 whole token in a class and cannot be subdivided."* [27]

This requirement derives from an industry technical taxonomy (the InterWork Alliance Token Taxonomy Framework) rather than from a regulatory authority, and is included as a technical reference; regulators do not directly address minimum-unit mechanics, but faithful tokenization of indivisible assets depends on them.

(28) Token Burning. Mechanisms for permanently removing tokens from circulation, for example on retirement, default, or supply reduction.

> *"A fungible parent token that can mint new tokens and a non-fungible child token that cannot, both classes of tokens are transferable."* [28]

(30) Asset Class Management. Support for different regulatory requirements based on asset classification.

> *"Recommendation 12: Regulators should set the expectation that CASPs should keep accurate and up-to-date customer asset records and accounts that readily establish the exact nature, amount, location and ownership status of the customer assets. Records should also be kept in a way that they could be used as an audit trail."* [13]

> *"53. Digital assets that are unique and not interchangeable, and that in practice are used as collectibles rather than as payment or investment instruments, may be referred to as non-fungible tokens (NFTs) or crypto-collectibles. Such assets are generally not considered VAs under the FATF definition depending on their characteristics."* [4]

(31) Token Supply Control. Mechanisms for controlling token supply through minting and burning.

> *"A fungible parent token that can mint new tokens and a non-fungible child token that cannot, both classes of tokens are transferable."* [28]

As with Requirement 27, this requirement derives from an industry technical taxonomy (the InterWork Alliance Token Taxonomy Framework) rather than from a regulatory authority, and is included as a technical reference.

3.10 Requirements Coverage Matrix

The following matrix maps how existing token standards cover RCP's requirements, judged against each standard's base specification. A check mark (Yes) indicates the standard provides a base-specification mechanism addressing the requirement; a blank indicates it does not. The 1400 family and ERC-3643 are substantial, purpose-built security token standards, and ERC-7943 (the uRWA interface) is a recent, deliberately minimal enforcement interface; this matrix is not a judgement of any standard's quality, but a map of where each provides an on-chain mechanism for a given regulatory requirement, where it does not, and where a requirement is inherently off-chain.

This matrix assesses the 29 core regulatory requirements (Requirements 1 through 18, 20 through 28, and 30 through 31). Requirements 19 (Code Security) and 29 (Gasless Support) are non-normative implementation recommendations and are addressed under Implementation Recommendations in the Rationale section; they are not assessed here.

Coverage is assessed against each standard's base specification (for the 1400 family this includes its constituent draft sub-standards; for ERC-3643, its mandatory identity layer; for ERC-7943, the uRWA interface assessed as deployed over a fungible, ERC-20-style base token), excluding optional extensions and implementation-specific compliance modules. Because ERC-7943 is an interface layered on a base token rather than a standalone token, its three ledger-level rows (ledger immutability, transaction finality, and tokenized-cash issuance) are provided by that base and match the ERC-20 column, while the freeze, forced-transfer, and transfer-gating rows are provided by the uRWA interface itself. This assessment revises the analysis in the RCP reference where base-specification capabilities differ from it. This matrix is a point-in-time reference, not a conformance test: each standard's specification may be revised by its maintainers, and coverage may vary with implementation choices and subsequent updates. It is offered as a starting point, and readers are encouraged to propose corrections in the discussion thread. Several requirements (for example, suspicious-transaction monitoring and external audit support) are inherently operational or off-chain and are not expected to be met at the token-contract level by any standard.

#	RCP Requirement	ERC-20	ERC-7943	1400 family	ERC-3643
1	Customer Identity Verification				✓
2	Suspicious Transaction Monitoring				
3	KYC Change Detection				✓
4	Contract Version Tracking			✓	✓
5	Transaction History by Asset Type				
6	External Audit Support				
7	Role-Based Permissions			✓	✓
8	Asset Freeze		✓	✓	✓
9	Asset Recovery		✓	✓	✓
10	Trading Restrictions		✓	✓	✓
11	Transaction Limit				
12	Transaction Cancel or Modify				

#	RCP Requirement	ERC-20	ERC-7943	1400 family	ERC-3643
13	Pausing of Trading			✓	✓
14	Smart Contract Suspension				✓
15	Blacklist Management				
16	Forced Liquidation		✓	✓	✓
17	Personal Information Privacy				✓
18	Financial Transaction Privacy				
20	Ledger Immutability	✓	✓	✓	✓
21	Transaction Finality	✓	✓	✓	✓
22	Legal Document Attachment			✓	
23	Token Expiration				
24	Token Transfer Restrictions		✓	✓	✓
25	Tokenized Cash Issuance	✓	✓	✓	✓
26	Tokenized Securities Issuance			✓	✓
27	Decimal Unit Control				
28	Token Burning			✓	✓
30	Asset Class Management			✓	
31	Token Supply Control			✓	✓

Over the 29 assessed requirements, ERC-20 addresses 3, ERC-7943 addresses 8, the 1400 family addresses 16, and ERC-3643 addresses 18. ERC-7943 concentrates entirely on enforcement chokepoints: it standardizes freeze, forced transfer, and transfer gating, but its single forced-transfer primitive is deliberately neutral as to legal effect, so it cannot by itself record whether a given forced transfer is a recovery, a confiscation, or a liquidation. That is precisely the distinction RCP's action vocabulary supplies. ERC-3643 and the 1400 family cover the majority of the on-chain enforcement and identity requirements, yet none of those mechanisms records on-chain which legal effect it carries; the counts measure what a standard can do, not whether what it does is legally legible. The load-bearing signal in this matrix is therefore not the totals but two patterns: rows left blank across every standard (token expiration, transaction limits, financial-transaction privacy) mark defects no deployed standard resolves, and a single mechanism receiving a check under several legally distinct actions (ERC-7943's one forced transfer under both recovery and liquidation) shows the conflation the vocabulary is meant to name. Any cross-chain recognition of compliance status is a further gap that future Standards Track work would address.

---

4 Rationale

4.1 The Five-Principle Structure

The five-principle organization reflects how regulatory requirements functionally cluster:

1. Who participates (Traceability).
2. What is protected (Privacy).
3. How authorities intervene (Enforceability).
4. When finality occurs (Finality).
5. What properties must be preserved in tokenized assets (Tokenizability).

This structure describes existing regulatory organization rather than prescribing new categories.

4.2 Regulatory Action Differentiation

A key insight from regulatory analysis is that enforcement actions are not interchangeable. The legal distinction between asset freeze (temporary, reversible) and confiscation (permanent, ownership transfer) requires different on-chain mechanisms. Current standards providing only general transfer functions cannot adequately support regulatory compliance.

Differentiation is also a transparency and safety property, not only a legal one. Collapsing all enforcement into a single opaque transfer function hides the legal effect of an action; naming distinct actions makes on-chain enforcement legible, auditable, and bounded, so that an irreversible action such as confiscation cannot be executed under the appearance of a reversible one such as a freeze.

An enforcement action also carries an issuing authority, and where several authorities have jurisdiction over one asset their orders can conflict or require ranking. A shared action vocabulary is the layer at which authority and precedence can be named and reasoned about, even though resolving competing authorities remains a matter for implementations and for jurisdiction-specific legal process.

4.2.1 State Transition Dynamics

The taxonomy is not a flat list of labels; the actions induce a state transition system, and the reversibility and finality attributes of the taxonomy table are precisely the shape of that system. RCP records this dynamics so that a standard can describe not only which actions it supports but how those actions compose. A note on scope is needed first, because the transition view and the six-action vocabulary count actions differently, and the difference is deliberate. To express reversibility as a checkable property of the state machine, the reversal of each reversible action is represented as its own transition (UNFREEZE out of FROZEN, RELEASE out of SEIZED, UNRESTRICT out of RESTRICTED); the transition system therefore ranges over seven action labels rather than the six vocabulary terms. Conversely, RECOVER and LIQUIDATE do not appear as transitions here: they are force-transfer operations (a restorative transfer and an external-market liquidation) rather than regulatory state changes, and are modelled at a different layer. What remains, over the regulatory states {ACTIVE, FROZEN, SEIZED, CONFISCATED, RESTRICTED}, is a partial transition function; the following matrix records which transitions carry a defined legal meaning (• a defined transition, blank an undefined one). It is a reference for the legal shape of the actions, not a prescribed implementation.

from \ action	**(1)**	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**	**(7)**
ACTIVE	•		•		•	•	
FROZEN		•	•		•		
SEIZED				•	•		
RESTRICTED	•				•		•
CONFISCATED							

Actions: (1) FREEZE, (2) UNFREEZE, (3) SEIZE, (4) RELEASE, (5) CONFISCATE, (6) RESTRICT, (7) UNRESTRICT.

Regulatory state transition matrix. A • marks a defined transition from the row state under that action (numbered as in the legend above); a blank cell an undefined one. Each action leads to a single target state: FREEZE to FROZEN, SEIZE to SEIZED, CONFISCATE to CONFISCATED, RESTRICT to RESTRICTED, and the reversals UNFREEZE, RELEASE, and UNRESTRICT to ACTIVE.

Two structural properties follow from the legal semantics and are worth stating explicitly, be-

cause they are what a reversibility claim actually means at the level of the state machine. First, confiscation is terminal: it transfers ownership permanently, so no action is defined out of CONFISCATED. Writing the partial transition function as $\delta(\text{state}, \text{action})$, this is

$$\delta(\mathsf{CONFISCATED}, a) = \bot \quad \text{for every action } a$$

(no outgoing transition). Second, confiscation is universally reachable: from any state s other than CONFISCATED,

$$\delta(s, \mathsf{CONFISCATE}) = \mathsf{CONFISCATED} \quad \text{for all } s \neq \mathsf{CONFISCATED}.$$

The blank cells are equally deliberate: no transition is defined from SEIZED to FROZEN, because a seizure is a strictly stronger restraint than a freeze and is not relaxed into one directly, and none from FROZEN to RESTRICTED, because a general halt is lifted through ACTIVE before a conditional limitation is imposed. Undefined transitions are rejections with a legal rationale, not omissions.

The finality attribute of the taxonomy table induces a partial order on the deprivation actions, reflecting the escalation recognized in the cited frameworks (a freeze is provisional, a seizure is interim custodial, a confiscation is final):

$$\mathsf{FREEZE} \prec \mathsf{SEIZE} \prec \mathsf{CONFISCATE} \approx \mathsf{LIQUIDATE}.$$

RESTRICT and RECOVER lie outside this ladder: RESTRICT is a configurable, ownership-preserving limitation, and RECOVER is restorative rather than a deprivation. This ordering is descriptive of the legal frameworks RCP compiles; it is not a claim of total severity ranking, and the procedural criteria for each step remain a matter for the relevant jurisdiction. The internal consistency of this transition model has been mechanically checked in Isabelle/HOL; the machine-checked sources build from the `Oraclizer/formal-verification` repository (a build entry point is provided and the development is free of `sorry`, so the model is checkable end to end) and are written up in a companion paper [30].

4.3 Classification

This proposal is Standards Track in the ERC category because it standardizes an application-level convention: the shared meaning of the enforcement actions that token standards already expose. It specifies the vocabulary and the legal effect associated with each action, not the interface through which those actions are exposed; concrete interfaces remain the province of the standards that implement them.

Three properties follow from that choice. The taxonomy defines legal effect rather than implementation interfaces, so standards may express the same action through different mechanisms. Different jurisdictions may require different subsets of the requirements. And the conceptual framework can remain stable while implementations evolve.

This specification defines conformance requirements for any standard, implementation, or tool that claims conformance to the RCP action vocabulary, while leaving implementation mechanisms to the standards that adopt RCP. Those requirements are conditional: a standard that makes no such claim incurs no obligation, and no on-chain interface is imposed on any implementation. RCP constrains the meaning of a compliance claim, not whether any standard makes one.

Because RCP is a controlled vocabulary rather than a rule, it is insulated from regulatory churn: when a specific obligation changes, the legal concepts it names, the reversibility and ownership effect of a freeze versus a confiscation, do not. What may require periodic revision is the requirements base, which is explicitly dated, non-exhaustive, and open to amendment through the discussion thread; the normative taxonomy is expected to remain stable.

4.4 Neutrality and Non-Endorsement

RCP confers no authority and creates no obligation. It documents regulatory positions that competent authorities have already published; it does not endorse, rank, or assert the legitimacy of any particular enforcement action, authority, or jurisdiction's legal regime. The decision of which authorities to recognize, and whether any action is lawful, rests entirely with implementations and with the off-chain legal processes of the relevant jurisdiction. Publication of this proposal should not be read as establishing regulatory compliance as a protocol-level objective of Ethereum: it standardizes only the meaning of the terms used to describe enforcement actions, and it binds only those standards that claim conformance to that vocabulary.

The authors of this EIP build tokenization and regulatory-compliance infrastructure and therefore have a commercial interest in this area. RCP is offered as shared, vendor-neutral reference material for the community, not as a mandate, an endorsement of any author's products, or a claim of authority over how standards adopt it. Its value rests on the regulatory sources it compiles and the vocabulary it defines, both of which are open to public scrutiny and correction.

4.5 Relationship to Existing Standards

A standard relates to RCP by reference, not by import: RCP defines no interface and contributes no code, so a referencing standard incurs no dependency and remains usable exactly as before. A standard that chooses to reference RCP can:

- Describe its coverage in common terms: state which RCP requirements it addresses, using shared vocabulary rather than standard-specific prose.
- Name the legal effect of its operations: map a function such as a forced transfer onto an RCP action (for example RECOVER or CONFISCATE), making explicit the reversibility and ownership effect that the mechanism alone does not express.
- Declare conformance to the action vocabulary: state that the distinct actions it supports are represented as distinct, separately observable operations.

In each case RCP supplies a layer of legal meaning over a standard's existing mechanism; it does not change, replace, or constrain that mechanism. Other Standards Track proposals may reference these definitions in this way. This proposal does not prescribe specific implementations.

4.6 Relationship to Minimal Enforcement Primitives

Recent Standards Track work, notably ERC-7943 (the uRWA universal Real World Asset interface, which recently reached Final) alongside the established ERC-3643, converges on a single neutral enforcement primitive: a forced transfer that deliberately omits the legal motivation of the action. RCP is complementary to this approach rather than competing with it. It supplies the legal-effect vocabulary, distinguishing a reversible freeze from an irreversible confiscation, that such a primitive does not by itself express. That even a finalized, adopted interface leaves this legal effect unstated is not a shortcoming of the interface (the omission is deliberate and correct for a neutral primitive) but precisely the definitional gap RCP fills. A future Standards Track EIP could map RCP's regulatory action taxonomy onto a minimal primitive of this kind, recording which legal effect a given forced transfer represents while leaving the on-chain mechanism unchanged.

4.7 Implementation Recommendations

The following are non-normative technical recommendations for implementations seeking to maximize compliance functionality. They are documented here for consistency with the original RCP

research numbering (Requirements 19 and 29) but are not regulatory requirements and are not assessed in the Requirements Coverage Matrix.

4.7.1 Gasless Transaction Support (Requirement 29)

For regulatory actions requiring immediate execution regardless of token holder gas availability, implementations should consider:

- Meta-transaction support for regulatory authority addresses (for example, the trusted-forwarder pattern of ERC-2771).
- Relayer networks for time-sensitive enforcement actions.
- Pre-funded gas pools for emergency freeze operations.

This enables regulatory authorities to execute enforcement actions without relying on third-party gas provision.

4.7.2 Code Security (Requirement 19)

Code security represents a software development best practice applicable to all smart contract systems rather than a security-token-specific regulatory mandate. While regulatory guidance from authorities such as MAS and the EU references IT and cyber security considerations, implementations should consider:

- Formal verification of critical contract logic.
- Independent security audits before deployment.
- Bug bounty programs for ongoing vulnerability discovery.
- Upgradeable contract patterns with appropriate governance controls.

4.8 Policy Considerations

Contributed by Dan Spuller, Executive Vice President of Industry Affairs, Blockchain Association (USA).

4.8.1 The Distinction Between "Can" and "Must"

The Regulatory Compliance Protocol (RCP) is best understood as a conceptual framework. While it defines standardized actions such as FREEZE, SEIZE, and RECOVER, these functions are intended to serve as common rails for reflecting the outcomes of external legal determinations on-chain. The protocol itself does not grant, delegate, or adjudicate regulatory authority. The authorization of any enforcement action remains an off-chain legal process, initiated through valid due process within a specific jurisdiction. The on-chain execution of those lawfully authorized decisions will be specified in the corresponding Standards Track EIP. The existence of a technical capability to pause or restrict a transaction does not, on its own, create a legal obligation to do so.

4.8.2 Modular Compliance for a Fragmented World

There is no single global rulebook for digital asset regulation. This EIP synthesizes guidance from multiple regulatory authorities to establish a shared vocabulary, but it does not define a one-size-fits-all compliance mandate. The framework is designed to support rigorous jurisdiction-specific requirements, and its real strength is that it does so without forcing those standards onto markets operating under different legal regimes. Regulatory obligations are inherently

local. What a platform operator must implement in one jurisdiction may differ materially from obligations in another. This framework is intentionally modular, allowing participants to map jurisdiction-specific legal requirements to common technical primitives without asserting a single, global compliance truth.

4.8.3 Privacy as a Functional Requirement

Regulatory oversight and traceability are important, but they cannot come at the expense of fundamental data protection. The RCP treats privacy-preserving technologies, such as zero-knowledge proofs and selective disclosure—not as optional add-ons, but as a preferred approach for meeting compliance objectives. The goal is to enable systems where an asset can demonstrate satisfaction of a regulatory condition without unnecessarily exposing sensitive information about the holder.

4.9 References

The following sources are cited by bracketed number throughout this document. Citations are provided as plain-text references to the publishing authority, document title, and year.

References

[1] World Bank (2020). Distributed Ledger Technology and Secured Transactions.

[2] FINMA (2023). Anti-Money Laundering Ordinance (AMLO-FINMA).

[3] HKMA (2017). Whitepaper 2.0 on Distributed Ledger Technology.

[4] FATF (2021). Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers.

[5] BIS-IOSCO (2012). Principles for Financial Market Infrastructures (PFMI).

[6] SFC (2023). Guidelines for Virtual Asset Trading Platform Operators.

[7] MAS (2021). Technology Risk Management Guidelines.

[8] BIS (2020). Central Bank Digital Currencies: Foundational Principles and Core Features.

[9] FATF (2012-2023). International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations.

[10] FINRA (2017). Distributed Ledger Technology: Implications of Blockchain for the Securities Industry.

[11] ESMA (2022). Report on the DLT Pilot Regime (ESMA70-460-111).

[12] FCA (2023). FG23/3: Finalised Guidance on Cryptoasset Financial Promotions.

[13] IOSCO (2023). Policy Recommendations for Crypto and Digital Asset Markets.

[14] FINRA (2021). FINRA Rules.

[15] EU (2022). DLT Pilot Regime (Regulation (EU) 2022/858).

[16] IOSCO (2010). Objectives and Principles of Securities Regulation.

[17] EU (2016). General Data Protection Regulation (GDPR).

[18] EU (2014). Markets in Financial Instruments Directive II (MiFID II).

[19] ISDA (2019). Legal Guidelines for Smart Derivatives Contracts: Introduction.

[20] EU (2023). Data Act (Regulation (EU) 2023/2854).

[21] EU (2014). Markets in Financial Instruments Regulation (MiFIR).

[22] IMF-FSB (2023). Synthesis Paper: Policies for Crypto-Assets.

[23] ISDA (2019). Legal Guidelines for Smart Derivatives Contracts: Collateral.

[24] ESMA (2024). Consultation Paper on the Draft Guidelines on the Conditions and Criteria for the Qualification of Crypto-Assets as Financial Instruments (ESMA75-453128700-52).

[25] IOSCO (2017). Research Report on Financial Technologies (Fintech).

[26] IOSCO (2019). Crypto-Asset Trading Platforms.

[27] InterWork Alliance (2020). Token Taxonomy Framework: Specification.

[28] InterWork Alliance (2020). Token Taxonomy Framework: Overview.

[29] Kim, J. and Hong, J. (2026). A Regulatory Compliance Protocol for Asset Interoperability Between Traditional and Decentralized Finance in Tokenized Capital Markets. arXiv:2603.29278.

[30] Kim, J. (2026). Safety and Liveness of Cross-Domain State Preservation under Byzantine Faults: A Mechanized Proof in Isabelle/HOL. arXiv:2604.03844.

---

5 Backwards Compatibility

This proposal introduces no backwards compatibility issues. It defines no interface and creates no code dependency, so existing standards and deployments are unaffected. Existing and future standards may voluntarily reference this protocol. Standards such as ERC-20 and ERC-3643 remain fully usable; RCP provides a vocabulary and a coverage reference against which any standard may be assessed.

---

6 Security Considerations

6.1 Regulatory Authority Management

Implementations must protect regulatory authority designation. Compromise of authority credentials could enable unauthorized asset freezes, malicious blocking of transactions, and false compliance reporting. Recommended mitigations include multi-signature schemes, timelocks, and transparent authority registries. Authority key rotation and revocation should be supported, with a defined treatment of in-flight and already-executed actions when a key is rotated or revoked.

6.2 Authority Abuse and Over-Reach Resistance

Beyond compromise of authority credentials, a framework that standardizes enforcement actions must consider authorized but wrongful or overly broad action, where a legitimate key is used incorrectly or too widely. Implementations and the Standards Track work that builds on this framework should:

- Emit an auditable on-chain event for every enforcement action, recording the action type, the acting authority, and the affected scope.

- Minimize the scope of each action, preferring per-asset or per-holder measures over contract-wide measures where the legal order permits.
- Provide a defined challenge, appeal, and reversal path, using the reversibility of actions such as FREEZE and RECOVER as a safety property rather than only a legal one.

Bounding and making enforcement legible in this way is itself a mitigation, since it constrains the blast radius of a wrongful action and prevents an irreversible action from being executed under the guise of a reversible one.

6.3 Privacy and Compliance Balance

The protocol acknowledges tension between privacy (the Privacy principle) and oversight (the Traceability principle). Traceability requirements specify what regulatory oversight must be able to establish, not that identity or transaction history must be publicly exposed; the Privacy principle constrains how that oversight is provided. Implementations should use privacy-preserving techniques where possible while maintaining regulatory compliance capability. Approaches include:

- Zero-knowledge proofs for compliance verification without data exposure.
- Selective disclosure mechanisms through cryptographic commitments.
- Trusted execution environments for confidential computation with audit capability.
- View key architectures enabling regulator access without public exposure.
- Homomorphic encryption for computing compliance checks over encrypted data.

6.4 Cross-Chain Considerations

Cross-chain compliance verification introduces attack surfaces including:

- False proofs from compromised bridges.
- Race conditions between regulatory actions on different chains.
- State inconsistencies due to finality differences.
- Partial application of an enforcement action across chains, leaving a window in which the same asset remains transferable on chains where the action has not yet taken effect.
- Replay of a regulatory-action message authorized for one chain or epoch onto another chain, or its re-execution after a chain reorganization. Implementations should bind each action to a chain identifier or domain separator and a nonce, and should account for reorganizations on chains whose finality is probabilistic.

These considerations should be addressed in Standards Track implementations that build on this framework.

6.5 Regulatory Authority Hierarchy

When multiple regulatory authorities have jurisdiction over the same asset (for example, a court order in one jurisdiction and a sanctions designation in another), their actions can conflict, and the on-chain layer must record whose action executed. RCP does not define a precedence order among authorities and does not rank them: the relative authority of any two orders (for example, a national court order and an international body's guidance, or a primary as opposed to a secondary sanctions measure) is a matter of the applicable law, conflict-of-laws rules, and comity, and is not fixed by any protocol. Implementations should therefore:

- Attribute every enforcement action to a named issuing authority on-chain, so that conflicting or superseding actions are auditable.
- Defer the resolution of competing authorities to the off-chain legal process that governs them, rather than encode a fixed priority in the contract.
- Provide explicit, auditable governance for recording which action took effect when orders conflict.

Copyright