EIP-XXXX: Regulatory Compliance Protocol for Tokenized Assets

Informational

Field	Value
eip	XXXX
title	Regulatory Compliance Protocol for Tokenized Assets
description	A protocol defining regulatory compliance requirements for tokenized asset interoperability across jurisdictions and blockchain networks
author	Jinwook Kim (@jay-oraclizer), Rob Viglione, Dan Spuller
discussions-to	https://ethereum-magicians.org/t/eip-xxxx-regulatory-compliance-protocol/xxxxx
status	Draft
type	Informational
created	2025-12-18

1 Abstract

This EIP introduces the Regulatory Compliance Protocol (RCP), a comprehensive protocol for systematically classifying regulatory requirements for tokenized assets in capital markets. Through systematic review of guidance documents from 15 global financial regulatory authorities, RCP consolidates 31 core requirements organized under five fundamental principles: Traceability, Privacy, Enforceability, Finality, and Tokenizability. This protocol serves as a foundational reference for security token standards seeking regulatory compliance and establishes a common vocabulary necessary for cross-chain and cross-jurisdictional interoperability of tokenized assets.

---

2 Motivation

2.1 The Interoperability Problem

The tokenization of real-world assets presents significant opportunities for capital market efficiency. However, this potential is constrained by a fundamental gap: the absence of a unified regulatory compliance protocol that enables tokenized assets to operate across different blockchain networks and regulatory jurisdictions.

Currently, tokenized assets exist as isolated systems. A tokenized bond on one network cannot meaningfully interact with tokenized securities on another without manual verification of compliance status, regulatory standing, and identity requirements. This fragmentation limits capital efficiency and contradicts the core value proposition of distributed ledger technology.

2.2 The Interoperability Prerequisite

Consider a practical scenario: an ERC-1400 security token on Chain A needs to interact with an ERC-3643 compliant token on Chain B. How does Chain B verify the regulatory compliance status of the incoming asset?

Without a common compliance protocol:

- There is no standardized way to query compliance status
- There is no common vocabulary for regulatory actions
- There is no mechanism to verify that freeze/seize actions are honored across chains

This is not merely inconvenient—it is a **structural impossibility**. Regulatory compliance interoperability requires standardization as a **prerequisite**, not an optimization.

RCP addresses this by providing:

1. A common vocabulary for compliance status
2. Standardized taxonomy of regulatory actions
3. A protocol for cross-chain compliance verification

2.3 Gaps in Existing Standards

The Ethereum ecosystem has produced security token standards including ERC-1400 and ERC-3643. While these represent important progress, they address only portions of regulatory requirements without a unified conceptual framework.

ERC-1400 Ecosystem:

- Fragmented across sub-standards (ERC-1594, ERC-1410, ERC-1643, ERC-1644)
- Provides a single `controllerTransfer` function insufficient for distinguishing legally distinct regulatory actions
- No mechanism for cross-chain compliance status verification
- Remains in Draft status since 2018

ERC-3643:

- Designed for single-chain, single-jurisdiction scenarios
- Identity management coupled to specific implementations
- Limited support for diverse asset classes with varying regulatory requirements

Common Gaps:

- No token expiration mechanisms (essential for bonds, derivatives)
- No standardized regulatory action taxonomy
- No cross-chain compliance verification
- No unified identity framework balancing privacy with regulatory oversight

2.4 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 regulatory positions, not interpretive frameworks.

---

3 Specification

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 and RFC 8174.

3.1 Regulatory Authorities Reviewed

This protocol incorporates requirements from the following 15 authorities:

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

Note: This protocol also includes technical references from industry standard bodies (e.g., InterWork Alliance/Token Taxonomy Framework), which are classified separately as industry standards rather than regulatory authorities.

3.2 The Five Principles

RCP organizes 31 regulatory requirements under five principles derived from functional analysis of regulatory frameworks.

3.3 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.

3.3.1 Requirements

(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]

> *"A financial institution is expected to perform KYC processes as part of its on-boarding process before conducting business with a new customer... 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]

> *"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/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]

> *"8.1 A platform operator should establish and implement written policies and controls for proper surveillance of trading activities on its trading platform to identify, prevent and report any market manipulative or abusive trading activities."* [6]

> *"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.

> *"A. 1. When in the course of establishing or during a customer relationship, or when conducting an occasional transaction, a financial institution suspects the transaction relates to money laundering or terrorist financing, the institution should: (a) normally seek to identify and verify the identity of the customer and the beneficial owner, whether permanent or occasional, and irrespective of any exemption or any designated threshold that might otherwise apply."* [9]

> *"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

Contract version tracking is needed for audit and compliance purposes.

> *"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]

> *"149. ESMA considers that amendments under the transaction reporting regime rely on the fact that transaction report items are sequential (i.e., 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]

(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]

> *"9.33 A platform operator should provide each of its clients with timely and meaningful information about the transactions conducted by or for the client, the client's virtual asset and fiat currency holdings and movements, and other activities on the client's account."* [6]

> *"Chapter 7: Recommendations on the custody of customer funds and assets - 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]

> *"2.56 Proof of ownership of the underlying commodity or assets, for example through disclosure, independent audits or proof of reserves. Firms should make evidence of the underlying commodity or assets accessible through the customer journey before a potential consumer makes an investment."* [12]

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

> *"10.6. Accounting and auditing standards: Accounting 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]

3.4 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 principles.

3.4.1 Requirements

(7) Setting Role-Based Permissions

Access control based on roles and responsibilities must be implemented.

> *"9 Access Controls - 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]

> *"Article 6(2)(a) Internal monitoring bodies, in particular the compliance function and internal audit, and, where applicable, the group audit firm, must have access to all information on individual business relationships of all branches and group companies."* [2]

> *"(63) Where possible the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data."* [17]

(17) Privacy of Personal Information

Personal information must be protected according to data protection principles.

> *"Interpretive Note to Recommendation 40 - A. 2. Countries should not prohibit or place unreasonably restrictive conditions on the provision of exchange of information or assistance. 4. Competent authorities should maintain appropriate privacy for any request for cooperation and the information exchanged, consistent with both parties' obligations concerning privacy and data protection to protect the integrity of the investigation or enquiry."* [9]

> *"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') - 1. 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 following grounds applies."* [17]

(18) Privacy of Financial Transactions

Financial transaction data requires appropriate privacy protections.

> *"Interpretive Note to Recommendation 40 - A. 2. Countries should not prohibit or place unreasonably restrictive conditions on the provision of exchange of information or assistance. 4. Competent authorities should maintain appropriate privacy for any request for cooperation and the information exchanged."* [9]

> *"12300. Submission of Documents and Service - 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."* [10]

> *"Chapter 5: Recommendations on addressing abusive conduct - 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]

(19) Code Security

Security of smart contract code and system infrastructure is required.

> *"(41) A DLT market infrastructure should have in place specific and robust IT and cyber arrangements related to the use of distributed ledger technology. Such arrangements should be proportionate to the nature, scale and complexity of the business plan of the operator of the DLT market infrastructure. Such arrangements should also ensure the continuity and ongoing transparency, availability, reliability and security of services provided."* [15]

> *"Annex 4: Details of organisational requirements according to Article 16 of MiFID II - i) have sound security mechanisms in place to guarantee the security and authentication of the means of information transmission, minimise the risk of data corruption and unauthorised access and to prevent information leakage maintaining the privacy of the data at all times."* [11]

3.5 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 (e.g., ERC-1644's `controllerTransfer`), which is insufficient for distinguishing legally distinct actions.

3.5.1 Requirements

(8) Asset Freeze

Regulators require the ability to temporarily halt transactions on specific assets.

> *"D. Preventive measures - 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]

> *"Interpretive Note to Recommendation 4 - C. 4. In response to relevant information, countries should enable the FIU or other competent authorities to take prompt action to withhold or suspend consent, directly or indirectly, to a transaction suspected of being related to money laundering, a predicate offence, or TF. The maximum duration of this measure should be specified and allow enough time for the transaction to be analysed and for competent authorities to initiate freeze or seizure action if appropriate."* [9]

> *"Part III: Application of the FATF Standards to Countries and Competent Authorities - 116. Recommendation 6. Countries should also freeze without delay the funds or other assets—including VA—of designated persons or entities, and ensure that no funds or other assets—including VA—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]

(9) Asset Recovery

Mechanisms for recovering assets in cases of fraud, theft, or court orders.

> *"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]

> *"Part V: Country Case Studies on Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers - 346. US departments and agencies have taken robust civil and criminal enforcement actions against illicit activities involving digital assets in administrative proceedings and federal courts, including seeking a variety of forms of relief including injunctions and cease and desist orders, disgorgement with prejudgment interest, civil penalties for willful violations, and criminal penalties including forfeiture and imprisonment."* [4]

(10) Trading Restrictions

Authority to impose restrictions on trading activity.

> *"2300. Special Products - 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 Algorithmic trading - 2. 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."* [18]

> *"XI. Management, Supervision and Internal Controls - 11.13 A platform operator should have effective risk management and supervisory controls for operation of its trading platform. These controls should include the following: (a) (ii) preventing the platform from immediately accepting suspicious client orders."* [6]

(11) Transaction Limit

Setting limits on transaction amounts or frequency.

> *"Interpretive Note to Recommendation 10 - H. 22. The designated threshold for occasional transactions under Recommendation 10 is USD/EUR 15,000. Interpretive Note to Recommendation 16 - B. 5. Countries may adopt a minimum threshold (no higher than USD/EUR 1,000) for cross-border wire transfers."* [9]

> *"266. Recommendation 10 also describes scenarios in which FIs should undertake CDD measures, including in the context of establishing a business relationship, carrying out occasional transactions above a designated threshold (USD/EUR 1,000 for VA transactions)."* [4]

> *"IX. Dealings with Clients - 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.

> *"Payments and deliveries - 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]

> *"Article 36 Essential requirements on smart contracts for the execution of data sharing agreements... That a mechanism exists to terminate the continued execution of transactions, and that the smart contract includes internal functions that can reset or instruct the contract to stop or interrupt the operation, to avoid future accidental executions in particular."* [20]

(13) Pausing of Trading

Authority to pause trading activity platform-wide or for specific assets.

> *"Article 9 Waivers for non-equity instruments - 4. 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]

"VII. Operations - 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]

"Chapter 5: Recommendations on addressing abusive conduct - Controls for taking prompt corrective action upon the discovery of market abuse on the platform (e.g., halting trading)." [13]

(14) Suspension or Disposal of Smart Contract (Kill Switch)

Authority to suspend or terminate smart contract operation.

"Article 36 Essential requirements on smart contracts for the execution of data sharing agreements... (b) safe termination and interruption, that a mechanism exists to terminate the continued execution of transactions, and that the smart contract includes internal functions that can reset or instruct the contract to stop or interrupt the operation, to avoid future accidental executions in particular; (c) data archiving and continuity, in order to keep records of the operations performed on the data in the past in situations where the smart contract must be terminated or deactivated, ensuring the possibility to archive the transactional data, the smart contract logic and code (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. VASPs should conduct their own risk-based assessment to determine if additional mitigating or preventive measures are warranted when there is a positive match." [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." [10]

(16) Forced Liquidation

Authority for forced liquidation of positions under specific circumstances.

"4200. Margin - 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: (i) 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; (ii) a proceeding in which a trustee, receiver or liquidator for such debtor has been appointed is pending before a court or agency of the United States or any State." [14]

> *"Principle 13: Participant-default rules and procedures - 3.13.4. A CCP should have rules and procedures that enable the prompt liquidation or transfer of a defaulting participant's proprietary and customer positions. In general, the longer these positions remain on a CCP's books, the greater the CCP's potential credit exposure, given changes in market prices or other factors. A CCP should have the capacity to apply the proceeds from liquidation, along with the other funds and assets of the defaulting participant, to fulfil the defaulting participant's obligations."* [5]

> *"3. A comprehensive policy and regulatory response - 3.3.4. Some authorities may consider implementing broad-based restrictions, targeted or time-bound, to manage the risks of crypto-assets."* [22]

3.5.2 Regulatory Action Taxonomy

Current standards provide limited regulatory action capability. However, regulatory actions have distinct legal meanings requiring differentiation:

Action	Description	Reversibility	Ownership
FREEZE	Temporary transaction halt	Reversible	Retained
SEIZE	Custody transfer to authority	Conditional	Retained
CONFISCATE	Permanent ownership transfer	Irreversible	Transferred
LIQUIDATE	Forced conversion for debt	Irreversible	Terminated
RESTRICT	Conditional trading limitations	Configurable	Retained
RECOVER	Return to rightful owner	One-time	Restored

Compliant implementations MUST distinguish between these actions as they have different legal implications and procedural requirements. A single `controllerTransfer` function cannot adequately represent these distinct regulatory mechanisms.

3.6 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.

3.6.1 Requirements

(20) Immutability of the Ledger

The integrity and immutability of the distributed ledger must be maintained.

> *"A mutual distributed ledger or blockchain has the following core functions: Ledger - 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]

> *"4 Use of DLT for trading and settlement - 30. Key stated benefits for the increased uptake of DLT-based solutions for financial market use raised by respondents include the following areas: 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]
>
> *“If some of the information relating to a transaction is subsequently changed as a result of either tampering or transmission error, for example the exact amount of a transaction, the algorithm executed on the changed block will no longer produce the correct hash and will therefore report an error.”* [3]

(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]
>
> *“Annex D: Summary of payment system, SSS, and CCP design - 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. In some systems, a payment is irrevocable as soon as the system validates it (that is, a queued payment order cannot be cancelled by the sender). However, a payment may not provide funds irrevocably and unconditionally to the payee or beneficiary until settlement occurs and is final.”* [5]
>
> *“11800. Clearance Procedures - 11870. (c) (1) (E) The carrying member and the receiving member shall promptly resolve and return non-transferable assets that were not properly identified during the verification. In all instances each member shall promptly update its records and book systems and notify the customer of action taken.”* [14]
>
> *“D. Preventive measures - 16. Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.”* [9]

(22) Attaching Legal Documents

Legal documents must be attachable and verifiable.

> *“5100. Securities Offerings, Underwriting and Compensation - 11500. Delivery of Securities with Restrictions - 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]
>
> *“Annex F Innovative Application of Laws to Facilitate DLT - In relation to digitalisation of original documents for DLT, general law / practice / procedures apply regardless of whether the context is DLT or otherwise. Generally, a digitalised version cannot receive the same legal status as the original, non-digitalised version, although this is more a question of admissibility / weight as evidence in court proceedings.”* [3]
>
> *“Disputes - It will also be important for both technology developers and derivatives market participants to consider new types of disputes that could arise as a result of entering into smart derivatives contracts. For example, it will 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]

3.7 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), classification properties, and restrictive properties (transfer limitations).

3.7.1 Requirements

(23) Token Expiration Time

Tokens representing time-bound assets must support expiration mechanisms.

> *"2300. Special Products - 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. The term 'expiration date' in respect of all other option contracts means the date specified therein."* [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 must have automatic principal repayment and token burn mechanisms.

(24) Token Transfer Restrictions

Tokens must support configurable transfer restrictions based on regulatory requirements.

> *"5100. Securities Offerings, Underwriting and Compensation - 5110. (g) (1) Other than in a public equity offering by an issuer that meets the requirements of subparagraph (b)(7)(C) or (ii) acquired unregistered by the underwriters and related persons prior to 180 days from the date of the required filing, including common or preferred stock of the issuer, options, warrants and other equity securities, debt securities convertible or exchangeable to equity securities..."* [14]

> *"6 Annexes - 109. Crypto-assets can be designed in such a way that does not allow for any transferability in the capital market. Some restrictions may be imposed to negotiability by not allowing the holder to negotiate and/or transfer the crypto-asset to anyone other than the issuer. In relation to restrictions to transfer of financial instruments, these should be considered case by case, and the nature and effect of the restriction may be sufficient to render an instrument non-tradable."* [24]

(25) Issuance of Tokenized Cash

Standards for representing cash or cash-equivalent instruments as tokens.

> *"Chapter 5: Distributed Ledger Technology (DLT) - 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.

> *"Chapter 1 - Summary - 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]

> *"6 Annexes - 134. National competent authorities and market participants should consider that, to be unique, an NFT should be considered distinguishable and non-fungible if it has characteristics and/or rights that are not the same as another crypto-asset(s) issued by the same (or different) issuer."* [24]

(27) Controlling Transactions Involving Splitting Below Decimal Units

Control over minimum trading units and decimal precision.

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

Note: IWA (InterWork Alliance) is an industry standard body, not a regulatory authority. This reference is included as a technical standard reference.

(28) Token Burning

Mechanisms for permanently removing tokens from circulation.

> *"4200. Margin - 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: (i) 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 - 3.13.4. A CCP should have rules and procedures that enable the prompt liquidation or transfer of a defaulting participant's proprietary and customer positions."* [5]

(30) Asset Class Management

Support for different regulatory requirements based on asset classification.

> *"Chapter 7: Recommendations on the custody of customer funds and assets - 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. Records should also be kept in a way that they could be used as an audit trail."* [13]

> *"Part II: Scope of the FATF Standards - 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.

> *"The Benefits of Shared Token Standards - TTF is more than just a list of definitions... A fungible parent token that can mint new tokens and a non-fungible child token that cannot, both classes of tokens are transferable."* [28]

Note: IWA (InterWork Alliance) is an industry standard body, not a regulatory authority. This reference is included as a technical standard reference.

3.8 Requirements Coverage Matrix

The following matrix compares requirements coverage across existing standards:

Note on Coverage Assessment: This matrix represents an analysis based on publicly available documentation as of December 2024. Coverage assessments may vary based on specific implementation choices and subsequent standard updates. Community feedback through the discussion forum is welcome.

Note on Numbering: Requirement 29 (Gasless Support) has been moved to Appendix A as it represents a technical implementation recommendation rather than an explicit regulatory requirement. Therefore, this matrix includes requirements 1-28 and 30-31.

#	RCP Requirement	ERC-20	ERC-777	ERC-1400	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/Modify	–	–	–	–
13	Pausing of Trading	–	–	✓	✓
14	Smart Contract Suspension	–	–	–	–
15	Blacklist Management	–	–	–	–
16	Forced Liquidation	–	–	–	–
17	Personal Information Privacy	–	–	–	–
18	Financial Transaction Privacy	–	–	–	–
19	Code Security	–	–	–	–
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	✓	✓	✓	✓
29	Gasless Support	–	–	–	–

#	RCP Requirement	ERC-20	ERC-777	ERC-1400	ERC-3643
30	Asset Class Management	–	–	–	–
31	Token Supply Control	✓	✓	✓	✓

Note: This table shows how existing token standards address the requirements defined by RCP. Some requirements, such as external audit support and personal information privacy, may require off-chain infrastructure.

---

4 Rationale

4.1 The Five Principles Structure

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

1. **Who participates** (Traceability)
2. **What is protected** (Privacy)
3. **How can authorities intervene** (Enforceability)
4. **When does finality occur** (Finality)
5. **What properties must be preserved in tokens** (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.

4.3 Informational Classification

This proposal is Informational rather than Standards Track because:

1. **Foundational nature**: Defines requirements rather than implementation interfaces
2. **Implementation flexibility**: Multiple standards can implement these requirements differently
3. **Jurisdictional adaptability**: Different jurisdictions may require different subsets
4. **Stability**: Conceptual framework can remain stable while implementations evolve

4.4 Relationship to Existing Standards

This framework provides:

- **Common vocabulary**: Standardized definitions for compliance terminology
- **Completeness reference**: Protocol for assessing standard coverage
- **Interoperability foundation**: Shared requirements enabling cross-standard compatibility

Future Standards Track EIPs may implement these principles. This Informational EIP does not prescribe specific implementations.

---

5 Backwards Compatibility

As an Informational EIP, this proposal introduces no backwards compatibility issues. Existing and future standards may voluntarily reference this protocol.

---

6 Security Considerations

6.1 Regulatory Authority Management

Implementations must protect regulatory authority designation. Compromise of authority credentials could enable:

- Unauthorized asset freezes
- Malicious transaction blocks
- False compliance reporting

Recommended mitigations include multi-signature schemes, timelocks, and transparent authority registries.

6.2 Privacy vs. Compliance Balance

The protocol acknowledges tension between privacy (Privacy) and oversight (Traceability). 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

6.3 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

These considerations should be addressed in Standards Track implementations.

6.4 Regulatory Authority Hierarchy

When multiple regulatory authorities have jurisdiction over the same asset, conflict resolution mechanisms are needed. Implementations should consider:

- Priority ordering based on authority level (international > national > regional)
- Temporal ordering for conflicting actions
- Explicit governance for authority disputes

---

7 Policy Considerations

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

7.1 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.

7.2 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.

7.3 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.

---

8 Acknowledgments

This research was developed in collaboration with Oraclizer Labs and Horizen Labs.

We welcome feedback from the Ethereum community and regulatory compliance practitioners.

References

[1] World Bank. (2021). Distributed Ledger Technology and Secured Transactions.

[2] FINMA. (2018). Special Regulations for Financial Intermediaries.

[3] HKMA. (2021). Distributed Ledger Technology White Paper.

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

[5] BIS-IOSCO. (2021). Application of the Principles for Financial Market Infrastructures to Stablecoin Arrangements.

[6] SFC. (2019). Statement on Security Token Offerings.

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

[8] BIS. (2021). Central Bank Digital Currencies: Foundational Principles and Core Features.

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

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

[11] ESMA. (2020). Advice on Initial Coin Offerings and Crypto-Assets.

[12] FCA. (2019). Guidance on Cryptoassets.

[13] IOSCO. (2020). Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms.

[14] FINRA. (2021). FINRA Rules.

[15] EU. (2022). Regulation on Markets in Crypto-Assets (MiCA).

[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. (2022). Data Act.

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

[22] IMF-FSB. (2023). Crypto-Asset Policy Implementation Framework.

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

[24] ESMA. (2022). Consultation Paper on Guidelines on Certain Aspects of the MiCA Suitability Requirements.

[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.

A Implementation Recommendations

The following are technical recommendations for implementations seeking to maximize compliance functionality, not regulatory requirements.

A.1 Gasless Transaction Support

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

- Meta-transaction support for regulatory authority addresses
- 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.

Note: This recommendation (gasless support) represents a technical implementation enhancement rather than an explicit regulatory authority requirement. It is documented here for consistency with the original RCP research numbering (Requirement 29) but is not assessed in the requirements coverage matrix.

A.2 Code Security

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 SEC references code 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

This ensures robust protection against exploits but is documented here as a general technical requirement that applies broadly to blockchain development rather than a compliance obligation unique to tokenized securities.

Note: This recommendation (code security) represents a software development best practice rather than an explicit regulatory authority requirement. It is documented here for consistency with the original RCP research numbering (Requirement 19) but is not assessed in the requirements coverage matrix.

Copyright