Consultation Paper

AFSA-P-CE-2023-0006

Proposed Astana International Financial Centre Security Token Offering Framework

Unrestricted

11 August 2023

Introduction

Why are we issuing this Consultation Paper (CP)?

1. The Astana Financial Services Authority (AFSA) has issued this Consultation Paper to seek suggestions from the market on the Policy paper and proposed AIFC Security Token Offering Framework.

Who should read this CP?

2. The proposals in this paper will be of interest to current and potential AIFC participants dealing with Security Tokens as well as the market and other stakeholders.

Terminology

3. Defined terms have the initial letter of the word capitalised, or of each word in a phrase. Definitions are set out in the AIFC Glossary (GLO). Unless the context otherwise requires, where capitalisation of the initial letter is not used, the expression has its natural meaning.

What are the next steps?

4. We invite comments from interested stakeholders on the proposed framework. All comments should be in writing and sent to the address or email specified below. If sending your comments by email, please use "Consultation Paper AFSA-P-CE-2023-0006" in the subject line. You may, if relevant, identify the organisation you represent when providing your comments. The AFSA reserves the right to publish, including on its website, any comments you provide, unless you expressly request otherwise. Comments supported by reasoning and evidence will be given more weight by the AFSA.

5. The deadline for providing comments on the proposed framework is **15 September 2023**. Once we receive your comments, we shall consider if any refinements are required to this proposal.

6. AFSA prefers to receive comments by email at consultation@afsa.kz or posted to:
   Policy and Strategy Division
   Astana Financial Services Authority (AFSA)
   55/17 Mangilik El, building C3.2, Astana, Kazakhstan

Structure of this CP

Part I – Background;
Part II – Issues and Risks;
Part III – Benefits;
Part IV – Best Practice;
Part V – Proposals;
Part VI – Public Consultation Questions;
Annex 1 – Draft Amendments to AIFC Financial Services Framework Regulations (FSFR);
Annex 2 – Draft Amendments to AIFC Glossary (GLO);
Annex 3 – Draft Amendments to AIFC Authorised Market Institutions Rules (AMI);
Annex 4 – Draft Amendments to AIFC Market Rules (MAR); and
Annex 5 – Draft Amendments to AIFC Conduct of Business Rules (COB).

Background

1. A Security Token represents a distinct class of assets and its issuance process, the security token offering (STO), represents a unique method of financing ventures. A Security Token is a digital representation of an investment product, recorded on a distributed ledger, subject to regulation under securities laws. Tokenisation is the process of recording claims on real or financial assets that exist on a traditional ledger onto a programmable platform.
2. Current Security Token projects commonly use distributed ledger technology (DLT). A distributed ledger (DL) is a record of transactions held across a network of computers (nodes) where each node has a synchronised copy. A DL usually relies on cryptography to allow nodes to securely propose, validate and record state changes (or updates) to the synchronized ledger without necessarily the need for a central authority.
3. According to BIS Quarterly Review[1], there are a few distinctions between book-entry and tokenised securities:
   1) Verification Process:
      - for book-entry securities, transfer authorisation ultimately depends on the Central Securities Depositary (CSD) verifying the identity of the account holder;
      - for digital tokens authorisation depends on “validation” of the token.
   2) Degree of centralization:
      - a CSD is highly centralized, which means that there can be only one entity that updates the central ledger and sees all transaction histories;
      - DLT platforms for tokenised securities exhibit different degrees of decentralization.
4. The global market for STOs is still in its nascent stages, but it is expected to see significant growth in the next few years, as the regulatory landscape becomes clearer, and more businesses and investors become aware of the benefits of STOs.
5. STOs can provide businesses with access to capital and a global pool of investors, while investors can benefit from liquidity, diversification, and transparency. However, STOs are subject to regulatory scrutiny and compliance requirements.
6. Tokenising securities on a DLT has the potential to reduce some of the costs and complexities in clearing and settlement, but it is not without risks. Tokenisation does not change the underlying risks in the settlement cycle, but it may transform some of them and change how they are managed. It may also have implications for the role of intermediaries in securities clearing and settlement.
7. Development of the AIFC Security Token Offering Framework (the “STO Framework”) was prompted by the need to introduce appropriate regulatory regime for Persons undertaking activities that involve or relate to Security Tokens.

Issues and Risks

8. There are several regulatory issues surrounding security tokens that tend to arise:
   a) One of the primary regulatory challenges is determining whether security tokens fall under the definition of securities in a particular jurisdiction. If they are deemed to be securities, they

[1] "On the future of securities settlement," BIS Quarterly Review, Bank for International Settlements, March 2020

are subject to securities regulations, including registration, disclosure, and compliance requirements.

b) Regulatory frameworks for security tokens are often designed to protect investors. This might include rules regarding accredited investors (investors meeting certain financial criteria), investment limits, and providing investors with accurate and transparent information.

c) Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations are typically applicable to security token offerings. Issuers and platforms may need to verify the identity of their investors and ensure compliance with AML regulations.

d) Depending on the jurisdiction and the specific activities involved (issuing, trading, custody, etc.), entities dealing with security tokens may need to obtain specific licenses or approvals from regulatory bodies.

e) Security tokens can be traded globally, leading to challenges related to cross-border regulations and compliance. This involves understanding how different jurisdictions treat security tokens and ensuring compliance in all relevant regions.

f) Regulatory considerations extend beyond just the tokens themselves. The platforms and exchanges facilitating trading of security tokens may also need to adhere to specific regulations, such as market surveillance and fair trading practices.

g) Regulators need to understand the underlying blockchain technology, smart contracts, and other technical aspects to ensure that the regulatory framework appropriately addresses the unique features of security tokens.

9. Consequently, STOs are associated with the following important risks:

a) STOs are subject to securities laws, which means that businesses must comply with a complex and ever-changing regulatory environment, which can be costly and time-consuming.

b) STOs are a new and relatively untested investment product, and there is no guarantee that security tokens will hold their value.

c) STOs could be subject to greater regulation in the future, which could limit their usefulness as a fundraising tool.

10. Given that the regulatory landscape for security tokens is still evolving and considering the above-mentioned issues and risks, which need to be addressed, the AFSA considers crucial to develop the AIFC Security Token Offering Framework (the “STO Framework”) to introduce appropriate regulatory regime for Persons undertaking activities that involve or relate to Security Tokens.

Benefits

11. The STOs offer the following potential benefits that are widely acknowledged by industry experts:

a) STOs are compliant with securities laws and regulations, making them a secure investment option for both investors and issuers.

b) STOs can provide liquidity to investors, allowing them to sell their securities on a regulated secondary market.

c) Tokenisation has the potential to enhance the liquidity of certain financial assets, e.g., unlisted shares or syndicated loans, by making transfer of ownership easier and faster.

d) Tokenisation may also reduce the need for intermediaries.

e) DLT facilitates the use of smart contracts, which automate the execution of contract obligations, thereby potentially reducing risks and costs. This could in turn provide positive outcomes for both market participants and end-consumers.

f) DLT supports the wider distribution of ownership records and transaction histories. In principle, having a single ledger that is held by all parties reduces the need for reconciliation and confirmation of trade details between back offices post-trade.

g) The use of blockchain technology for STOs makes it possible to provide greater transparency, since investors can have access to real-time information about the investment and trading activity.

Best Practice

12. The AFSA has considered the international standard setting, particularly IOSCO, and have considered the numerous jurisdictions' regulatory approaches in relation to the Security Token. Our main goal was to determine whether Security Tokens are similar in nature to traditional assets and can therefore fit into the existing regulatory framework for securities.
13. According to IOSCO's recommendations, regulators may consider applying existing regulations that govern traditional financial instruments, such as securities, to certain crypto-assets if they are found to behave similarly to or act as substitutes for regulated financial instruments.
14. In addition, IOSCO's approach to retail investor participation in crypto-asset markets emphasizes the need for additional protections and requirements, including well-constructed suitability assessments, transparent disclosures, and efficient complaint handling mechanisms. These measures are intended to mitigate the unique risks posed by these markets and ensure that retail investors are adequately informed and safeguarded in their participation.
15. Some international regulatory authorities (European Securities and Markets Authority, FCA, BaFin, Financial Market Authority of Switzerland) have adopted a token classification dividing cryptoassets into three broad categories, typically:
    - Payment/exchange tokens or cryptocurrencies: a means of value exchange;
    - Utility tokens: granting access to a digital platform or service;
    - Security tokens: an investment instrument.

16. According to the Cambridge Centre for Alternative Finance's study a prevalent regulatory approach to date (82 % of 108 selected jurisdictions) is to draw a clear distinction between cryptoassets that qualify as securities and those that do not (please see Figure 1 below).

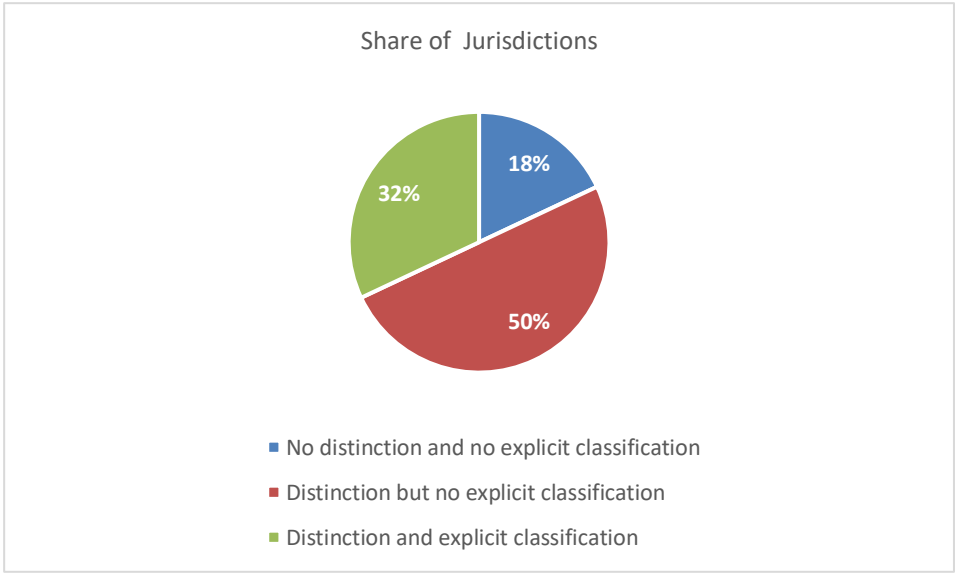

Figure 1: Regulatory approaches to cryptoasset classification

17. The regulatory developments of the following jurisdictions were analysed:

Dubai International Financial Centre ("DIFC")

18. In October 2021, the DFSA introduced the Investment Token Framework. The DFSA has adopted an approach that involves incorporating Investment Tokens within the existing regulatory framework for 'Investments,' instead of creating a completely separate regime. This approach required certain modifications to take into account the unique characteristics of investment tokens. For completeness it is noted that the definitions of investments is different from the way that the term is more broadly defined to include digital assets at the AIFC.
19. A Security Token is considered an Investment Token, which is either a Security or an instrument that confers rights and obligations similar to a Security, or has a purpose or effect comparable to a Security. It is important to note that this type of tokens fall under the broader category of Investment Tokens, which also includes Derivative Tokens.
20. In DIFC Security Tokens may be offered on both traditional exchange and multilateral trading facility (MTF)/organised trading facility (OTF) platforms. The DIFC approach to regulation of security tokens appears to be an important precedent for the AIFC, given the similar status of the financial centres and the treatment of security tokens within the existing regime for authorised market institutions.

Abu-Dhabi Global Market ("ADGM")

21. In ADGM, Security Tokens are defined as virtual tokens that have the features and characteristics of a Security under the FSMR (such as Shares, Debentures, Units in a Collective Investment Fund). Deemed to be Securities pursuant to Paragraph 58(2)(b) of FSMR. The ADGM has a high focus on promotion of the tokenisation regimes through their Multilateral Trading Platforms offering.
22. All financial services activities in relation to Security Tokens, such as operating primary/secondary markets, dealing, trading, managing investments in or advising on such tokens, will be subject to the relevant regulatory requirements under the FSMR.
23. Market intermediaries and market operators dealing or managing investments in Security Tokens need to be approved by FSRA as Financial Services Permission holders, Recognised Investment Exchanges or Recognised Clearing Houses, as applicable.
24. Where an Offer involves Retail Clients participation, it would qualify as an Exempt Offer if it is directed at no more than 200 Retail Clients, in circumstances where the Securities are offered within a Private Financing Planforms or Multilateral Trading Facilities.

Singapore

25. In Singapore, there is no specific regulatory regime applicable to security tokens. Security tokens are generally regulated in the same way as other types of traditional securities.
26. The Monetary Authority of Singapore (MAS) defines a Digital Token as a cryptographically-secured representation of a token-holder's rights to receive a benefit or to perform specified functions in several of its statements.

27. Offers or issues of digital tokens may be regulated by MAS if the digital tokens are capital markets products under the Securities and Futures Act. Capital markets products include any securities, units in a collective investment scheme, derivatives contracts, and spot foreign exchange contracts for purposes of leveraged foreign exchange trading.

The United Kingdom

28. The HM Treasury published its consultation on Future financial services regulatory regime for cryptoassets, which provides industry with an explanation of where cryptoassets interact with its regulatory perimeter. This consultation ran from 1 February 2023 to 30 April 2023.
29. Security tokens defined as cryptoassets which use a technology such as DLT to support the recording or storage of data and already meet the definition of a specified investment under the Financial Services and Markets Act 2000 and are therefore already subject to regulation.
30. The FCA already has powers to implement regulatory requirements for activities relating to security tokens , which meet the definition of a specified investment. Security tokens are allowed to be offered on a Regulated Market or a primary MTF.

Hong Kong

31. Under the Securities and Futures Ordinance (SFO) and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), centralised virtual asset trading platforms carrying on their businesses in Hong Kong, or actively marketing their services to Hong Kong investors, are required to be licensed and regulated by the Securities and Futures Commission (SFC).
32. Definition of “virtual assets” include any virtual asset and security token. Security token means a cryptographically secured digital representation of value which constitutes “securities” as defined in Chapter 571 of SFO.
33. Trading platforms intending to provide trading in security tokens need to be licensed under the Securities and Futures Ordinance (the SFO) for regulated activities Type 1 (dealing in securities) and Type 7 (providing automated trading services).
34. On June 1, 2023, Hong Kong implemented a new licensing regime for Virtual Asset Trading Platforms (VATPs). The VATP regime will operate in parallel with the SFO regime. VATPs engaging in the trading of security tokens will be regulated under the SFO, and those in the trading of non-security tokens under the VATP regime.
35. As required by its licensing conditions a Platform Operator should provide its security token trading services only to professional investors.

European Union

36. The EU treats security tokens as financial instruments, provided that they fall into the MiFID II definition. According to this definition, transferable securities qualify as financial instruments; the term ‘transferable securities’ is defined as follows:

    (a) shares in companies and other securities equivalent to shares in companies, partnerships or other entities, and depositary receipts in respect of shares;

(b) bonds or other forms of securitised debt, including depositary receipts in respect of such securities;

(c) any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures.

37. If security tokens meet the criteria outlined by MiFID II and fall within the scope of transferable securities, they are considered to be financial instruments under EU regulations.
38. The EU adopted a Pilot Regime for tokenized securities, which took effect on 23 March 2023 for an initial three-year period, extendable for an additional three years. The pilot regime allows for certain DLT market infrastructures to be temporarily exempted from some of the specific requirements of Union financial services legislation that could otherwise prevent operators from developing solutions for the trading and settlement of transactions in crypto-assets that qualify as financial instruments, without weakening any existing requirements or safeguards applied to traditional market infrastructures.
39. The DLT Pilot Regime allows for DLT trading and settlement systems and DLT MTFs to provide for direct retail participation with no broker intermediation.

Proposals

Approach to bringing Security Tokens within AFSA regulation.

40. After the analysis of various approaches to Security Tokens regulation, we can conclude that this type of Investment is already a subject to the existing AFSA Legal Acts since Security Tokens are similar in nature, effect or purpose to traditional Securities.
41. Therefore, we propose to cover the Security Tokens regulation within scope of the existing framework for Securities, subject to certain changes.
42. In light of the above consideration, we propose to extend the current definition of Security in the AIFC Glossary by defining Security Token as a digital representation of Security, that is issued, transferred and stored using DLT or other similar technology.

The type of Licence needed to operate a facility for trading and/or clearing Security Tokens.

43. Since the AFSA regulatory approach to Security Tokens proposed to be similar to Securities, we consider that our regulatory regime for Investment Exchanges, as well as for Clearing Houses should continue to apply to platforms that trade and/or clear Security Tokens.
44. Hence, Investment Exchange was selected as a primary platform for offering of Security Tokens rather than MTF/OTF, since it provides a controlled environment that can help maintain a certain level of investor protection and compliance.
45. Consequently, we propose to include in the AIFC GLO the definition of Operating a Facility for Security Tokens, which means Operating an Investment Exchange on which Security Tokens are traded and Operating a Clearing House on which Security Tokens are cleared.
46. Accordingly, a holder of an AMI licence will be permitted to operate an Investment Exchange for the trading of Security Tokens and Clearing House to clear and settle transactions in Security Tokens, subject to the additional requirements.

Access to facilities for trading and clearing Security Tokens

47. Nowadays, the platform solutions which offer reduced total transaction costs, expedited clearing and settlement cycles, as well as efficient post-trade reporting opportunities, are becoming a challenge for the traditional intermediated model.
48. We propose to allow a direct access of Persons to the facility on which Security Tokens are to be traded and cleared, which means that there would be no orders coming through the regulated firm. This allows direct access to buyers and sellers of Security Tokens on the platform, regardless of whether such buyers and sellers are retail or professional, or individual or institutional.
49. Table 1 below shows the main risks and benefits of allowing direct access to trading in Security Tokens:

Benefits	Risks
✓ No need for intermediation ✓ Enable issuers of securities to raise capital by making their offers of securities, using smart contracts and similar technologies, an automated process	✓ Systemic risks arising from large defaults would need to be addressed ✓ Market integrity risks are heightened in a direct market access model to trading ✓ AML/CTF risks are particularly significant, especially given the degree of anonymity that can be achieved in a completely automated, direct access environment

Table 1: Risk and benefits of direct access

50. However, an operator of a facility on which are to be traded will be required to demonstrate to the AFSA that it has adequate systems and controls to address market integrity, AML/CTF and investor protection risks.

Enhanced requirements for trading and clearing Security Tokens.

51. Considering that Security Token is a digital representation of Security an additional layer of regulation is needed to address issues and concerns relating to the use of DLT or similar technologies that underpin Security Tokens.
52. After preliminary analysis conducted by the AFSA, it is proposed to introduce the following requirements related to AMIs operating a facility for Security Tokens:
    1) Technology and governance requirements;
    2) Additional requirements applicable to AMIs operating a facility for Security Tokens that permits direct access;
    3) Safe custody of Security Tokens;
    4) Technology audit reports;
53. Also, it is proposed to the additional content information in the case of a Prospectus relating to a Security Token.
54. Considering direct market access in relation to trading and clearing of Security Tokens, the relevant provisions of AIFC COB Rules proposed to be applied to an AMI operating a facility for Security Tokens.

55. We propose that Authorised Firms who offer Financial Services to clients in respect of Security Tokens be required to, in addition to entering into a Client Agreement with such clients, provide to those clients a key features document relating to Security Tokens.

56. To implement the proposals above the following Act are subject to amendments set out in Annexes 1-5:

- AIFC Financial Services Framework Regulations (FSFR)
- AIFC Authorised Market Institution Rules (AMI)
- AIFC Market Rules (MAR)
- AIFC Conduct of Business Rules (COB)
- AIFC Glossary (GLO).

57. It is proposed to introduce additional fixed application and annual supervision fees for Authorised Market Institutions admitting Retail Clients as Direct Access Members in respect of trading and/or clearing of Security Tokens. The additional information on this proposal can be found in the Consultation Paper AFSA-P-CE-2023-0004 on proposed Amendments to the AIFC Fees Rules.

Public consultation questions

58. In the course of public consultation, existing and potential market participants will be invited to comment on the following questions:

(1) Do you agree with our proposal to treat Security Tokens as Securities and to extend the current definition of Security in the AIFC Glossary by defining Security Token as a digital representation of Security, that is issued, transferred and stored using DLT or other similar technology? If not, why not?

(2) Do you agree with our proposal to allow AMI operators to operate facilities to trade Security Tokens, subject to the additional requirements proposed in this paper? If not, why not?

(3) Do you agree with our proposals to allow only an AMI holding a licence to Operate a Clearing House to clear Security Tokens? If not, why not?

(4) Do you agree with our proposal to include in the AIFC GLO the definition of Operating a Facility for Security Tokens, which means Operating an Investment Exchange on which Security Tokens are traded and Operating a Clearing House on which Security Tokens are cleared? If not, why not?

(5) Do you agree with our proposal to allow a direct access of Persons to the facility on which Security Tokens are to be traded and cleared? If not, why not?

(6) Do you have any concerns related to the amendments proposed to introduce a new category of Members of AMI, Persons with access to the facility, on which Security Tokens are traded or cleared or both traded and cleared, in respect of only trading or clearing of Security Tokens?

(7) Should we confine direct access to trading in Security Tokens for Professional Clients only? If so, what are your reasons?

(8) Should we limit the participation of Retail Clients in these markets, as an investor protection measure, by placing limits on the volume of their trading activity? If not, why not?

(9) Do you agree that the AFSA considered all the main risks and benefits of allowing direct access to trading in Security Tokens? If not, what ae additional risks or benefits that can be included?

(10) Do you think that the term Security Token is appropriate if the token confers rights and obligations that are the same as, or similar in nature to, those conferred by Units? If not, should they be referred to as Unit Tokens? Please explain your thinking.

(11) Should the AFSA allow the conversion of Security tokens to Securities and vice-versa?
(12) Do you agree with our proposals to introduce the additional application and annual supervision fee for the AMIs dealing in Security Tokens?
(13) Do you agree with the proposed amendments to AIFC Rules and Regulations set out in Annexes 1-5? If not, what are your concerns, and how should they be addressed?
(14) Are there any other issues that need to be addressed regarding the regulation of Security Tokens? If so, what are they, and why and how should they be addressed?

Annex 1

SECURITY TOKEN OFFERING FRAMEWORK

Proposed amendments to the AIFC Financial Services Framework Regulations

In these Regulations, the underlying indicates a new text and the strikethrough indicates a removed text

(…)

55. Persons eligible for Membership

(1) Subject to such further admission criteria as the AFSA may prescribe by Rules, an Authorised Market Institution may only admit as a Member:

(a) an Authorised Firm; ~~or~~

(b) a Recognised Non-AIFC Member; ~~or~~

(c) a Person that is a Body Corporate which intends to undertake Commodity Derivative or Environmental Instrument transactions on the relevant Authorised Market Institution by carrying on such activities for its own account or for another Body Corporate which is in the same Group as the Person, provided that any such member of the Group for which the Person intends to act is a wholly-owned Subsidiary of a Holding Company within the Group or is the Holding Company itself; or

(d) a Person not referred to in (a),(b), and (c) with access to the facility, on which Security Tokens are traded or cleared or both traded and cleared, in respect of only trading or clearing of Security Tokens.

(…)

Annex 2

Proposed amendments to the AIFC Glossary

In these Rules, the underlying indicates a new text and the strikethrough indicates a removed text

2. INTERPRETATION

Security	1. A Security is: (a) a Share; (b) a Debenture; (c) a Warrant; (d) a Certificate; ~~or~~ (e) a Structured Product; or (f) a digital representation of rights and obligations in respect of (a), (b), (c), (d) or (e), that is issued, transferred and stored using DLT or other similar technology. 2. For the purposes of article 6 of the Constitutional Law, a Security shall be treated as if it includes a Unit.
Token	A digital representation of value, rights or obligations, which may be issued, transferred and stored electronically, using DLT or other similar technology.
Security Token	A digital representation of Security, that is issued, transferred and stored using DLT or other similar technology.

Operating a facility for Security Tokens	In relation to an Authorised Market Institution, means carrying on one or more of the following activities: (a) Operating an Investment Exchange on which Security Tokens are traded; (b) Operating a Clearing House on which Security Tokens are cleared.
Direct Access Member	In relation to an Authorised Market Institution, means a Person that the Authorised Market Institution admits as a Member in accordance with AMI 2.6.1 (1) (d).
Digital wallet Service Provider	An Authorised Firm Providing Custody of Security Tokens or Digital Assets by holding and controlling the public and private cryptographic keys relating to the Security Tokens or Digital Assets.

Annex 3

Proposed amendments to the AIFC Authorised Market Institutions Rules

In these Rules, the underlying indicates a new text and the strikethrough indicates a removed text

(…)

Guidance: Purpose and application of AMI

(…)

The application of the rules in AMI is as follows:

- Chapter 1 contains introductory provisions applicable to all Authorised Market Institutions.
- Chapter 2 contains rules and guidance applicable to all Authorised Market Institutions.
- Chapter 2-1 contains rules and guidance applicable to Authorised Market Institutions Operating a facility for Security Tokens.
- Chapter 3 contains additional rules and guidance applicable to Authorised Investment Exchanges.
- Chapter 4 contains additional rules and guidance applicable to Authorised Clearing Houses (including Authorised Central Counterparties).
- Chapter 5 contains rules in relation to the supervision of Authorised Market Institutions.
- ~~Chapter 6 contains additional rules and guidance applicable to Authorised Digital Assets Trading Facility.~~
- Chapter 7 contains additional rules and guidance applicable to Authorised Crowdfunding Platforms.

(…)

(1) **INTRODUCTION**

1.1. Introduction

1.1.1. Definitions

(1) An Authorised Market Institution is a Centre Participant which has been licensed by the AFSA to carry on one or more Market Activities. An Authorised Market Institution can be an Authorised Investment Exchange, ~~an Authorised~~

~~Digital Asset Trading Facility~~, an Authorised Clearing House and/or an Authorised Crowdfunding Platform.

(2) An Authorised Investment Exchange is a Centre Participant which has been licensed by the AFSA to carry on the Market Activity of Operating an Investment Exchange.

(3) An Authorised Clearing House is a Centre Participant which has been licensed by the AFSA to carry on the Market Activity of Operating a Clearing House.

(4) A central counterparty is a legal Person that interposes itself between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer.

(5) An Authorised Central Counterparty is a central counterparty which is declared by an order made by the AFSA under these Rules for the time being in force to be an Authorised Central Counterparty.

(6) A Member of an Authorised Market Institution is a Person who is entitled, under an arrangement or agreement between him and the Authorised Market Institution, to use that institution's facilities.

(7) ~~An Authorised Digital Asset Trading Facility is a Centre Participant which has been licensed by the AFSA to carry on the Market Activity of Operating a Digital Asset Trading Facility.~~

(8) An Authorised Crowdfunding Platform is a Centre Participant which has been licensed by the AFSA to carry on the Market Activity of Operating a Loan Crowdfunding Platform and/or Operating an Investment Crowdfunding Platform.

(9) Operating a Facility for Security Tokens in relation to an Authorised Market Institution means Operating an Investment Exchange on which Security Tokens are traded and Operating a Clearing House on which Security Tokens are cleared.

(…)

2.5.1. Requirement to prepare Business Rules

(…)

(2) An Authorised Market Institution must incorporate into its Business Rules the substance of any additional provisions to be found in the COB Rules, with any modifications which seem to the Institution to be appropriate, for the purpose of regulating the conduct of business of a Person referred to in AMI 2.6.1(1)(c) as a Member of the Institution for the purposes of dealing in Commodity Derivatives or Environmental Instruments.

(3) An Authorised Market Institution must incorporate into its Business Rules the substance of additional provisions to be found in the COB Rules, for the purpose of regulating the conduct of business of a Person referred to in AMI 2.6.1(1)(d) as a Member of the Institution for the purposes of dealing in Security Tokens.

(…)

2.6. Membership

2.6.1. Persons eligible for Membership

(1) An Authorised Market Institution, except an Authorised Digital Asset Trading Facility, may only admit as a Member a Person who satisfies admission criteria set out in its Membership Rules and who is categorised as either:

(a) an Authorised Firm whose Licence permits it to carry on the Regulated Activities of Dealing in Investments; ~~or~~

(b) a Recognised Non-AIFC Member;

(c) a Person intending to deal in Commodity Derivatives or Environmental Instruments who meets the criteria in GEN 1.1.14; or

(d) a Person not referred to in (a), (b), and (c) with access to the facility, on which Security Tokens are traded or cleared or both traded and cleared, in respect of only trading or clearing of Security Tokens.

(2) An Authorised Market Institution must ensure that a Member who is a Person referred to in (1)(c) is a Professional Client and treat the Person as such.

For the purposes of this rule, Professional Client has the same meaning as defined in COB Chapter 2.

(3) Before admitting a Person referred to in (1)(c) as a Member, an Authorised Market Institution must undertake due diligence to ensure that such a Person:

(a) is of sufficient good repute;

(b) has a sufficient level of competence, experience and understanding of relevant Investments, Financial Services, transactions and any associated risks, including appropriate standards of conduct for its staff permitted to use its order entry system; and

(c) has adequate organisational arrangements, including financial and technological resources, which are appropriate to allow it to discharge its obligations in respect of their category of membership at the Authorised Market Institution.

(4) An Authorised Market Institution must keep records of the procedures which it has followed under (3), including any documents that evidence the Person's assessment. The records must be kept for at least six years from the date on which the business relationship with a Person ended.

(5) Before admitting a Person referred to in (1)(d), an Authorised Market Institution must undertake due diligence to ensure that the Person:

(a) is of sufficient good repute;

(b) has a sufficient level of competence, experience and understanding of relevant Investments, Financial Services, transactions and any associated risks, including appropriate standards of conduct for its staff permitted to use its order entry system;

(c) has adequate financial and technological resources to meet the Business Rules of the facility; and

(d) does not pose any operational risks to the orderly and efficient functioning of the facility's trading or clearing systems.

(…)

2-1. RULES APPLICABLE TO AUTHORISED MARKET INSTITUTIONS OPERATING A FACILITY FOR SECURITY TOKENS

Guidance

Operating a facility for Security Tokens is defined in GLO as Operating an Exchange and Operating a Clearing House on which Security Tokens are traded, cleared, or both traded and cleared.

2-1.1. Technology and governance requirements

2-1.1.1. Without limiting the generality of the technology resources requirements in AMI 2.4, an Authorised Market Institution must:

(a) ensure that any DLT application used in connection with the facility operates on the basis of 'permissioned' access, such that it allows the operator to have and maintain adequate control over the Persons who are permitted to access and update records held on that DLT application;

(b) establish and maintain adequate measures to ensure that the DLT application it uses, and the associated rules and protocols, contain:

(i) clear criteria governing Persons who are permitted to access and update records for the purposes of trading or clearing Security Tokens on the facility, including criteria about the integrity, credentials and competencies appropriate to the roles played by such persons;

(ii) measures to address risks, including to network security and network compatibility, that may arise through systems used by Persons permitted to update the records on the DLT application; and

(iii) processes to ensure that the Authorised Market Institutions undertakes sufficient due diligence and adequate monitoring of ongoing compliance, relating to the matters referred to in (i) and (ii);

(c) ensure any DLT application used for its facility is fit for purpose; and

(d) have regard to industry best practices in developing its technology design and technology governance relating to DLT that is used by the facility.

Guidance

1. To be fit for purpose, the technology design of the DLT application used by an Authorised Market Institution Operating a facility for Security Tokens should be able to address how the rights and obligations relating to the Security Tokens traded on that facility are properly managed and capable of being exercised or performed. For example, where a Security Token confers rights and obligations substantially similar to those conferred by a Share in a company, the DLT application would generally need to enable the management and exercise of the shareholder's rights. These may, for example, include the right to receive notice of, and vote in, shareholder meetings, receive any declared dividends and participate in the assets of the company in a winding up.

2. To ensure the technology governance of any DLT application used on its facility is fit for purpose, an Authorised Market Institution should, as a minimum, have regard to the following:

a. careful maintenance and development of the relevant systems and architecture in terms of its code version control, implementation of updates, issue resolution, and regular internal and third party testing;

b. security measures and procedures for the safe storage and transmission of data in accordance with agreed protocols;

c. procedures to address changes in the protocol which result in the splitting of the underlying distributed ledger into two or more separate ledgers (often referred to as a 'fork'), whether or not the new protocol is backwards compatible with the previous version (soft fork) or not (hard fork), and access to information where such a fork is created;

d. procedures to deal with system outages, whether planned or not;

e. decision-making protocols and accountability for decisions;

f. procedures for the establishing and managing interfaces with providers of digital wallets; and

g. whether the protocols, smart contracts and other inbuilt features of the DLT application meet at least a minimum acceptable level of reliability and safety requirements, including to deal with a cyber or hacking attack, and how any resulting disruptions would be resolved.

2-1.2. Operating a facility for Security Tokens that permits direct access

2-1.2.1. An Authorised Market Institution must ensure that:

(1) it treats each Direct Access Member as its Client;

(2) its Business Rules clearly set out:

(a) the duties owed by the Authorised Market Institution to the Direct Access Member and how the Authorised Market Institution is held accountable for any failure to fulfil those duties; and

(b) the duties owed by the Direct Access Member to the Authorised Market Institution and how the Direct Access Member is held accountable for any failure to fulfil those duties;

(3) appropriate investor redress mechanisms are available, and disclosed, to each Member permitted to trade or clear Security Tokens on its facility; and

(4) its facility contains a prominent disclosure of the risks associated with the use of DLT for trading and clearing Investments, particularly those relating to Digital Wallets and the susceptibility of private cryptographic keys to misappropriation.

2-1.2.2. (1) Without limiting the generality of the systems and controls obligations of the Authorised Market Institution, an Authorised Market Institution must have in place adequate systems and controls to address market integrity, AML, CTF and investor protection risks in permitting a Direct Access Member to access its facility, including procedures to:

(a) identify the ultimate beneficial owner of a Direct Access Member, where the Member is a Body Corporate;

(b) ensure that appropriate customer due diligence sufficient to address AML and CTF risks has been conducted on each Direct Access Member, before permitting that Member to access its facility;

(c) detect and address market manipulation and abuse; and

(d) ensure that there is adequate disclosure relating to the Security Tokens that are traded on the facility, through prospectus and ongoing disclosure under chapters 1 and 6 of MAR.

(2) An Authorised Market Institution must have adequate controls and procedures to ensure that trading in Security Tokens by Direct Access Members does not pose any risks to the orderly and efficient functioning of the facility's trading system, including controls and procedures to:

(a) mitigate counterparty risks that may arise from defaults by Direct Access Members, through adequate collateral management measures, such as margin requirements, based on the settlement cycle adopted by the Authorised Market Institution;

(b) identify and distinguish orders that are placed by Direct Access Members, and, if necessary, enable the Authorised Market Institution to stop orders of, or trading by, such Members;

(c) prevent Direct Access Members from allowing any other Persons to access the facility through that Member's access; and

(d) ensure that Direct Access Members fully comply with the Business Rules of the facility and promptly address any gaps and deficiencies that are identified.

(3) An Authorised Market Institution must have adequate resources and mechanisms to carry out front-line monitoring of the trading activities of Direct Access Members.

(4) An Authorised Market Institution must ensure that, to the extent that any of the systems and controls referred to in (1) are embedded within, or otherwise facilitated through DLT, they must be included within the scope of the annual audit and written report required under AMI 2-1.5.

2-1.2.3. When an Authorised Market Institution Executes a Transaction in Security Tokens for a Direct Access Member, the Authorised Market Institution must comply with the requirements relating to confirmation notes that would apply to an Authorised Firm under COB 9.1.2, 9.1.3 and 9.1.5.

2-1.3. Safe custody of Security Tokens

2-1.3.1. Without limiting the generality of AMI 2.9, where an Authorised Market Institution's obligations include making provision for the safeguarding and administration of Security Tokens belonging to Members and other participants on its facility, it must ensure that:

(1) where its safe custody arrangements involve acting as a Digital Wallet Service Provider, it complies with the Client Asset provisions in COB 8.2 and 8.3 and the following requirements for firms Providing Custody of Security Tokens:

(a) Digital Wallet Service Provider must ensure that:
   (i) any DLT applications it uses in Providing Custody of Security Tokens are resilient, reliable and compatible with any relevant facility on which those Security Tokens are traded or cleared;
   (ii) it has the ability to clearly identify and segregate Security Tokens belonging to different Clients; and
   (iii) it has in place appropriate procedures to enable it to confirm Client instructions and transactions, maintain appropriate records and data relating to those instructions and transactions and to conduct a reconciliation of those transactions at appropriate intervals.

(b) A Digital Wallet Service Provider, in developing and using DLT applications and other technology to Provide Custody of Security Tokens, must ensure that:
   (i) the architecture of any Digital Wallets used adequately addresses compatibility issues and associated risks;

(ii) the technology used and its associated procedures have adequate security measures (including cyber security) to enable the safe storage and transmission of data relating to the Security Tokens;

(iii) the security and integrity of cryptographic keys are maintained through the use of that technology, taking into account the password protection and methods of encryption used;

(iv) there are adequate measures to address any risks specific to the methods of usage and storage of cryptographic keys (or their equivalent) available under the DLT application used; and

the technology is compatible with the procedures and protocols built into the Operating Rules or equivalent on any facility on which the Security Tokens are traded or cleared or both traded and cleared.

(2) where it appoints a Third Party Digital Wallet Service Provider to Provide Custody for SecurityTokens traded or cleared on its facility, that person is either:

(a) an Authorised Firm permitted to be a Digital Wallet Service Provider; or

(b) a firm that is regulated by a Financial Services Regulator to an equivalent level as that provided for under the AFSA regime for Providing Digital Wallet Services.

2-1.4. Technology audit reports

2-1.4.1. An Authorised Market Institution must:

(a) appoint a suitably qualified independent third party professional to:

(i) carry out an annual audit of the Authorised Market Institution's compliance with the technology resources and governance requirements that apply to it; and

(ii) produce a written report which sets out the methodology and results of that annual audit, confirms whether the requirements referred to in (i) have been met and lists any recommendations or areas of concern;

(b) submit to the AFSA a copy of the report referred to in (a)(ii) within 4 months of the Authorised Market Institution's financial year end; and

(c) be able to satisfy the AFSA that the independent third party professional who undertakes the annual audit has the relevant expertise to do so, including by reference to the due diligence undertaken by the Authorised Market Institution to satisfy itself of that fact.

Guidance

An Authorised Market Institution may appoint an Auditor to carry out the functions specified in (a)(i) and (ii), provided it has satisfied itself that Auditor has the relevant expertise required to do so.

(…)

Annex 4

Proposed amendments to the AIFC Market Rules

In these Rules, the underlying indicates a new text and the strikethrough indicates a removed text

(…)

SCHEDULE 1: REGISTRATION DOCUMENT*

(…)

* In the case of a Prospectus relating to a Security Token the Registration Document must include the additional content information set out in Schedule 4.

(…)

SCHEDULE 2: SECURITIES NOTE*

(…)

*In the case of a Prospectus relating to a Security Token the Securities Note must include the additional content information set out in Schedule 4.

(…)

SCHEDULE 4: ADDITIONAL CONTENT OF A PROSPECTUS FOR SECURITY TOKENS

1. A Person producing a Prospectus in relation to a Security Token must ensure that:

(a) the Prospectus contains:

(i) information specified in paragraph 2; and

(ii) a statement confirming the matters specified in paragraph 3 made by a suitably qualified independent third party professional, who has given consent under MAR 1.9.3 for that statement to be included in the Prospectus; and

(b) in the case of a Security Token which will be admitted to trading on an Authorised Market Institution, the Prospectus contains the information specified in paragraph 4.

2. The following information is specified for the purposes of paragraph 1(a)(i):

(a) the essential characteristics of the Security Token, including the rights and obligations conferred by it and details of the Person or Persons responsible for meeting such obligations and against whom such rights can be exercised;

(b) the type of Security which the Security Token constitutes and a clear analysis as to how the Security Token meets the definition of such type of Security;

(c) details of the Distributed Ledger Technology that is used to issue, store or transfer the Security Token;

(d) how the holder of a Security Token may exercise any rights conferred by it, such as voting or participation in shareholder actions;

(e) if the capital to be raised through issuing of the Security Token is to be used to fund the creation of a new Token, detailed information about:

(i) the project or venture to be funded;

(ii) whether it is the Issuer or a third party who will receive and apply the capital raised towards that project or venture (and if a third party, what rights and obligations a holder of the Security Token has in respect of that third party);

(iii) the features of that new Token and any rights and obligations attaching to it;

(iv) the terms and conditions relevant to the delivery or establishment of the project or venture, including any right of a Security Token holder to have their contribution refunded if any funding requirement is not met, the expected timetable for completion, any milestones included in that timetable and an explanation of the consequences if the timetable is not met; and

(v) the risks associated with the project or venture, including those associated with the technology used to deliver or facilitate its completion or the Token's ongoing use;

(f) how title to the Security Tokens is established, certified or otherwise evidenced;

(g) cybersecurity risks associated with the Security Token or its underlying technology, including whether there is a risk of loss of the Security Token in the event of a cyber attack, and details of steps that have been, or can be taken to mitigate such risks;

(h) details of other risks associated with the use of the DLT application, particularly those relating to Digital Wallets and the susceptibility of private cryptographic keys to misappropriation; and

(i) any other information relevant to the Security Token that would reasonably assist a prospective investor in making an informed decision about investing in the Security Token.

3. The matters to be confirmed in the statement referred to in paragraph 1(a)(ii) are that:

(a) the DLT application, used to issue, store or transfer the Security Tokens offered under the Prospectus, is an authentic, valid and workable solution capable of meeting its intended purpose; and

(b) the Prospectus accurately describes the architecture, functionality, effect, risks and vulnerabilities of the DLT application, including its compatibility with other technologies, applications and services with which it is intended to interact.

4. The following information is specified for the purposes of paragraph 1(b):

(a) details of a facility on which the Security Token is admitted to trading or cleared including:

(i) the Person responsible for operating an AMI;

(ii) details of each DLT application used by the operator to facilitate trading or clearing of the Security Token and the functionality provided by that DLT application;

(iii) details as to how the operator of the facility meets the technology and governance requirements set out in AMI 2-1.2;

(b) details of the custody arrangements for the Security Token that are permitted or required by the operator of facility, including, in respect of each such arrangement:

(i) the Person who carries out the function of the Digital Wallet service provider;

(ii) the Person who is responsible for the safe custody of the Security Token when held in the Digital Wallet; and

(iii) risks associated with the Digital Wallet, such as the consequences of the loss of cryptographic keys (private and public), cyber security risks associated with Digital Wallets held online, loss, theft or destruction of Digital Wallets held offline, and whether and how such risks are addressed;

(c) whether smart contracts are being used or executed on the facility and, if so:

(i) what form those smart contracts take;

(ii) how the legal rights and obligations arising under the smart contracts are performed, including when contract or settlement finality occurs, (whether by the smart contract itself, an underlying natural language contract or a combination of both); and

(iii) details of the relationship between those smart contracts and any underlying natural language contract.

Annex 5

Proposed amendments to the AIFC Conduct of Business Rules

In these Rules, the underlying indicates a new text and the strikethrough indicates a removed text

(…)

Guidance: Purpose of this rulebook

(…)

Chapter 1 (Application) states that the requirements in the COB rulebook generally apply to Authorised Firms licensed to carry on a Regulated Activity. Some requirements may be modified or disapplied altogether depending on the type of Authorised Firm involved, the nature of its activities, and/or the classification of the Client to whom the Authorised Firm provides services.

In particular, the majority of the COB rules do not apply to Insurance Intermediaries, Trust Service Providers, or Ancillary Service Providers, which are instead required to comply with the requirements set out in Chapters 11, 12 or 13 of COB respectively.

For the avoidance of doubt, COB does not apply to Representative Offices or Authorised Market Institutions, unless otherwise provided under Rules made by the AFSA.

(…)

1. APPLICATION

1.1. General application rule

The requirements in COB apply to an Authorised Firm with respect to any Regulated Activity carried on by an Authorised Firm operating within the jurisdiction of the AIFC as specified in Part 1 of the Framework Regulations.

(…)

1.2.2. Exclusions in relation to certain categories of Centre Participant

For the avoidance of doubt, the requirements in COB do not apply to:

(a) a Representative Office;

(b) an Authorised Market Institution (other than an Authorised Crowdfunding Platform ~~and an Authorised Digital Asset Trading Facility~~), except for COB 3 (Communications with Clients and Financial Promotions), unless otherwise provided under Rules made by the AFSA.

(…)

4. KEY INFORMATION AND CLIENT AGREEMENT

(…)

4.6. Provision of key features document relating to Security Tokens

(1) An Authorised Firm must not provide a Financial Service to which this section applies to a Person unless it has provided that Person with a key features document containing the information in (2).
(2) The key features document must contain the following information in respect of each Security Token relevant to the Financial Services that the Authorised Firm will provide to the Person:

(a) the risks associated with and essential characteristics of the Issuer (or other Person responsible for discharging the obligations associated with the rights conferred), and guarantor if any, of the Security Token, including their assets, liabilities and financial position;

(b) the risks associated with and essential characteristics of the Security Token, including the rights and obligations conferred and the type or types of Investment which it constitutes;

(c) whether the Security Token is or will be admitted to trading and if so, the details relating to such admission, including details of the facility and whether the facility is within the AIFC;

(d) whether the Client can directly access the trading facility, or whether access is only through an intermediary, and the process for accessing the facility;

(e) risks associated with the use of DLT, particularly those relating to Digital Wallets and the susceptibility of private cryptographic keys to misappropriation;

(f) whether the Client, the Authorised Firm or a third party is responsible for providing a Digital Wallet service in respect of the Security Token, and any related risks (for example, at whose risk the Client's Security Tokens are held in the Digital Wallet, whether it is accessible online or stored offline, what happens if keys to the Digital Wallet are lost and what procedures can be followed in such an event);

(g) how the Client may exercise any rights conferred by the Security Tokens such as voting or participation in shareholder actions; and

(h) any other information relevant to the particular Security Token that would reasonably assist the Client to understand the product and technology better and to make informed decisions in respect of it.

(3) The key features document must be provided in good time before the relevant Financial Service is provided to the Person, to enable that Person to make an informed decision about whether to use the relevant Financial Service.

(4) The key features document does not need to be provided to a Person to whom the Authorised Firm has previously provided that information, if there has been no significant change since the information was previously provided.

(…)