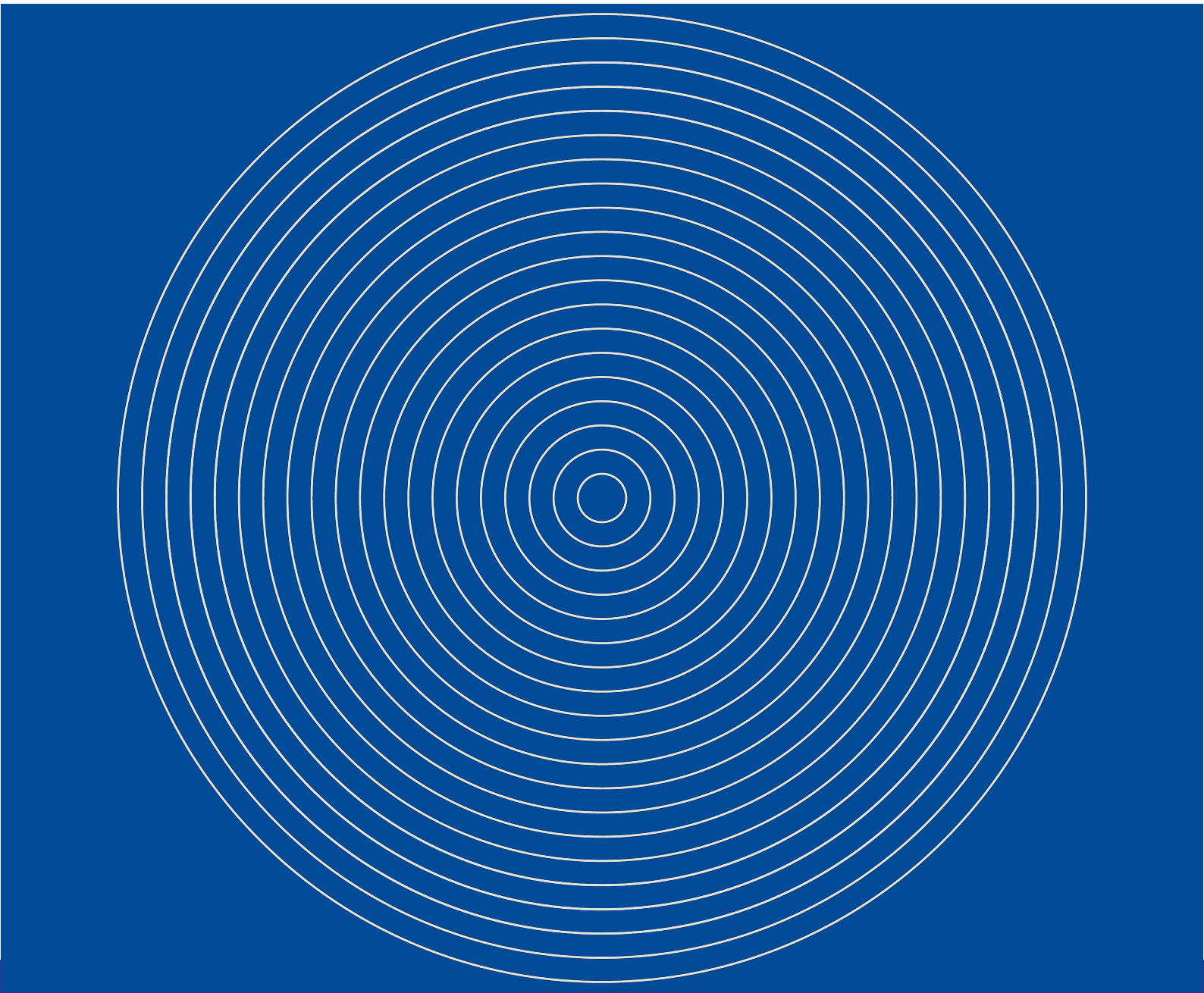
cmta.

Digital Assets - AML STANDARDS for Financial Intermediaries

September 2024



INTRODUCTION.

The Capital Markets and Technology Association (CMTA) is an independent Swiss association bringing together experts from the financial, technological, audit and legal sectors to promote the use of new technologies in capital markets. The CMTA provides a platform to create open industry standards around issuing, distributing and trading securities and other financial instruments in the form of "**Digital Assets**" using "**Distributed Ledger Technologies**" or "**DLT**".

As part of its mission, the CMTA has developed a set of standards for Digital Assets and the present document, as part of the standards series, is an updated version of the standards addressing AML policies and procedures for financial intermediaries that enter into business relationships with issuers, investors in Digital Assets ("**IDA**") or other types of clients whose business involves a material exposure to Digital Assets and/or DLT (the "**Standards**"). The reference to AML in these Standards includes a reference to CFT.

Entry into force	September 2024 The recommendations set out in these Standards apply to new relationships entered into by an Intermediary after the entry into force of these Standards or in situations where the due diligence or clarifications need to be repeated.
Legal framework (as of September 2024)	• Swiss Anti-Money Laundering Act (AMLA) • Swiss Anti-Money Laundering Ordinance (AMLO) • FINMA Anti-Money Laundering Ordinance (AMLO-FINMA) • FINMA Circular 16/7 "Video and online identification" • Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB 20) • FINMA Guidance 02/2019 "Payments on the blockchain"
Other source(s)	• SBA guidelines on opening corporate accounts for DLT companies published by the Swiss Bankers Association as updated in August 2019
Out of scope	The Standards do not address due diligence, documentation and compliance requirements or obligations of Intermediaries deriving from other Swiss or foreign legal or regulatory provisions, such as, without limitation: • sanctions and export controls; • tax or reporting requirements under the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS); • financial markets reporting; and • securities or other financial market laws and regulations.
Definitions	Available in Appendix A.

The application of the Standards is not mandatory and does not represent a binding minimum standard. However, the CMTA considers them as a practical toolkit that may, as a matter of example, be used by Intermediaries to develop their own risk-based approach as part of the implementation of their respective obligations in accordance with applicable laws and regulations in the field of AML compliance.

Although the core of the Standards aims to be technology-neutral to all possible extents, they need to be practical.

The CMTA may therefore, from time to time, proceed to adjustments and amendments of the Standards and publish revisions, additions or updates.

Any comments or suggestions for future updates may be addressed to the CMTA Secretariat by email to: admin@cmta.ch.

CMTA Digital Assets - AML Standards
for Financial Intermediaries

Version: 2.0
Published: September 10, 2024

Capital Markets and Technology Association
Route de Chêne 30
1208 Genève

admin@cmta.ch
+41 22 73 00 00

Table of contents

Table of Appendices

CHAPTER 1. INTRODUCTION

1. The Standards include a proposed risk-based approach for Intermediaries when performing AML due diligence checks:

   (a) upon entering into a relationship with different types of clients involved in or exposed to Digital Assets and/or DLT; and

   (b) as part of the ongoing monitoring of the relationship, in particular transactions.

   In addition, the Standards propose a set of procedures designed to implement the so-called "travel rule".

2. The Standards apply in addition to and not in lieu of applicable AML laws and regulations.

CHAPTER 2. BUSINESS RELATIONSHIP WITH AN ISSUER

1. This chapter describes the standards that a bank, securities firm or other Intermediary subject to AMLA may decide to apply when examining a request from an Issuer to enter into a business relationship and when performing its monitoring activities after entering into the business relationship.

Section 1. Know Your Issuer (KYI)

§ 1. Collection of relevant information

1. Issuers shall be required to complete a due diligence questionnaire (the "**DDQ-Issuer**"). The Intermediary may also complete the DDQ-Issuer on the basis of the information and documents provided by the Issuer.

2. The DDQ-Issuer shall cover the following information:

   (a) the Issuer, its management and its shareholders;

   (b) the business plan;

   (c) the Offering, whether it was already carried out, is in progress or is planned;

   (d) the Digital Asset(s) issued or to be issued;

   (e) the means of payment accepted by the Issuer as contribution for the acquisition of Digital Assets as part of the Offering;

   (f) the status of the Issuer and the Offering from a legal and regulatory perspective;

   (g) the Issuer's advisors and other persons involved in the business plan and Offering;

   (h) the general AML approach taken by the Issuer (e.g., due diligence tiers, list of Excluded Jurisdictions);

   (i) the manner in which AML requirements were, are or will be handled by the Issuer, in particular information on whether the following due diligence measures were or will be performed by the Issuer and with respect to which categories of Contributors:

      (1) check of the Contributor's identification document;

(2) check of a photograph of the Contributor taken during the identification process against the photograph on the identification document;

(3) verification of the identity by video-conference;

(4) check of the Contributor's proof of residence (e.g., utility bill);

(5) check of the Contributor's domicile address against the list of Excluded Jurisdictions;

(6) check of the Contributor's first and last name(s) against sanctions, politically exposed persons and adverse media databases;

(7) Blockchain Forensic Analysis of the Contributor's Public Wallet Address from which Digital Assets will be transferred;

(8) check of the contributor's IP address;

(9) verification of acceptability of the bank account of the Contributor (for contribution in Fiat Currency);

(10) check of the Contributor's source of funds;

(11) check of the Contributor's source of wealth;

(12) handling of multiple participations by the same Contributor.

(j) where applicable, the Issuer's compliance function and/or service provider in the field of AML; and

(k) where applicable, the Issuer's AML policy, guidelines, procedures or any other similar documents.

3. An example of DDQ-Issuer is enclosed as **Appendix B**.

4. Chapters 6 and 7 on Transaction Monitoring and Travel Rule respectively, apply in addition to Digital Asset transfers between an Issuer and the Intermediary.

§ 2. Identification of the Issuer as Contracting Party

1. The verification of the identity of the Issuer as the Intermediary's "**Contracting Party**" shall be performed in accordance with the AML requirements applicable to the Intermediary (e.g., CDB, SRO Regulations, and/or AMLO-FINMA). The same shall apply to the establishment of the identity of the controlling person(s) and the establishment of the identity of the beneficial owner(s) of the assets.

2. The Intermediary shall, for the purpose of the identification procedures, take into account the legal nature of the Issuer and whether the Issuer is the legal entity operating the business in question or not.

Section 2. Assessment and acceptance of business relationship

§ 1. Assessment of the information obtained

1. The Intermediary shall carefully review the information obtained and assess the level of due diligence requirements of the Issuer against:

(a) the AML requirements for Issuers which are subject to AMLA (e.g., Issuers of Digital Assets that are means of payment or "**Payment Tokens**" according to FINMA ICO Guidelines classification);

(b) the AML requirements applicable to the Intermediary (e.g., CDB, SRO Regulations, and/or AMLO/FINMA; and

(c) the current version of the Digital Assets – AML Standards for Issuers.

2. The Intermediary shall document the findings of the assessment, with explanations or comments for material discrepancies or derogations to the applicable minimum level of expected due diligence, in accordance with its risk-based approach policy.

§ 2. Acceptance of business relationship

1. Based on the outcome of the assessment and the risk appetite of the Intermediary, the Intermediary shall decide whether it approves the business relationship with the Issuer, depending on the Intermediary's risk-based approach.

2. The Intermediary shall define, according to a risk-based approach, criteria (e.g., thresholds, origin/background of Issuer, purpose of the business relationship, transaction patterns, target clients of the Issuer etc.) allowing to determine which business relationships with Issuers are to be classified as high risk relationships (HRR). Depending on its risk-based approach, an Intermediary may wish to categorize all relationships with Issuers as HRR, regardless of the purpose of the business relationship, or of the amounts concerned and/or any other criteria.

3. The decision of the Intermediary as regards the acceptance of a HRR shall be documented.

§ 3. Enhanced due diligence

1. In case of HRR Issuer or where the Intermediary deems it necessary, the Intermediary shall apply specific enhanced due diligence measures depending on its risk-based approach.

2. Depending on the circumstances, specific enhanced due diligence measures to be performed by the Intermediary may include the following:

   (a) performing a Wallet Ownership Verification ("**Wallet Ownership Verification**") on the Issuer's main Public Wallet Addresses and where applicable, on the Public Wallet Addresses from which Digital Assets will be transferred to the Intermediary;

   (b) performing controls (review) of the Blockchain Forensic Analysis previously carried out by the Issuer on Contributors' Public Wallet Addresses, if any;

   (c) requesting KYC information with respect to Contributors who acquired or signaled their willingness to acquire a significant percentage of the Digital Assets issued (e.g., 10% or more);

   (d) ordering an external due diligence report on the Issuer and/or its management and/or its shareholders; and/or

   (e) requesting detailed documentation on the legal nature of the Issuer (e.g., ruling from competent authorities or legal opinion).

Section 3. Periodic review and update of client file

1. The Intermediary shall perform a periodic review of client relationships with Issuers. The frequency and intensity of the review of the client relationship shall be determined on a risk-based approach, taking into account the nature of the business relationship with the Issuer, as well as the specific risk profile of the Issuer. By way of example, an Intermediary could choose to review the client relationship at least every two (2) years for normal risk relationships and every year for HRR.

2. The results of the review shall be documented.

3. In the event that any material changes are identified at any point in time, including as a result of a periodic review of

the client relationship, the Intermediary shall update the client file accordingly and take the appropriate measures.

CHAPTER 3. BUSINESS RELATIONSHIP WITH AN INVESTOR IN DIGITAL ASSETS

This chapter describes the standards that an Intermediary may decide to apply when examining a request to enter into a business relationship with an investor in Digital Assets and when performing its monitoring activities after entering into the business relationship.

Section 1. General provisions

§ 1. Definitions

1. Investors in Digital Assets ("**IDA**") are natural persons or entities who either:

   (a) hold financial assets which have been generated through investments in or transactions involving Digital Assets; or

   (b) contemplate transferring to the Intermediary or requesting services to be provided by the Intermediary in respect to Digital Assets.

2. Intermediaries should define relevant thresholds, depending on their respective business model, the financial services to be provided to the IDAs and client typology.

§ 2. Scope

1. The Standards set forth the minimum due diligence procedures applicable to:

   (a) the onboarding of IDA; and

   (b) existing business relationships that, during the course of the business relationship, are identified as IDA, as part of the ongoing monitoring of relationships or during periodic reviews.

2. Such minimum due diligence procedures are in addition to the applicable AML procedures to be performed by the Intermediary in application of, among others, AMLA, AMLO-FINMA, sanctions regimes and other applicable regulations.

Section 2. Inquiring on and verifying the source of wealth

§ 1. Generalities

1. The IDA shall be required to complete a due diligence questionnaire (the "**DDQ-IDA**"). The Intermediary may also complete the DDQ-IDA on the basis of the information and documents provided by the IDA.

2. The DDQ-IDA shall cover the following information:

   (a) information on the IDA's sophistication, knowledge and background in relation to Digital Assets and/or DLT;

   (b) total of the Fiat Currencies invested in Digital Assets;

   (c) origin of the Fiat Currencies invested in Digital Assets;

(d) exact or at least approximate date of the first investment(s) in Digital Assets;

(e) description of the IDA's holdings of Digital Assets, together with the planned use of such holdings (e.g., long term investments, payment for services);

(f) total current value of the IDA's holdings of Digital Assets;

(g) description and amount of the Digital Assets to be transferred to the Intermediary or in respect to which the Intermediary is to provide services, as applicable;

(h) list of the Public Wallet Addresses that contributed to the IDA's digital asset wealth;

(i) list of the Public Wallet Addresses from which the IDA intends to transfer Digital Assets to the Intermediary, if applicable;

(j) list of exchanges, brokers and platforms used to acquire, trade, sell and transfer Digital Assets and relevant account statements; and

(k) confirmation of compliance with local tax rules in regards to Digital Assets as per the tax compliance policy of the Intermediary.

3. In specific instances where one or some of the above information/documents are neither required nor relevant, the Intermediary may accept a prospect considered IDA for which one or some of the above inquiries are not answered.

4. An example DDQ-IDA is enclosed as **Appendix C**.

5. Chapters 6 and 7 on Transaction Monitoring and Travel Rule respectively, apply in addition to Digital Asset transfers between an IDA and the Intermediary.

§ 2. Enhanced due diligence

1. The Intermediary shall define, according to a risk-based approach, criteria (e.g., thresholds, origin/background of IDA, transaction patterns, etc.) on the basis of which the Intermediary will determine which business relationships with IDA are to be classified as high risk relationships (HRR). Depending on its risk-based approach, an Intermediary may decide to treat all relationships with IDA as HRR, regardless of the amounts involved and/or any other criteria.

2. A Blockchain Forensic Analysis shall be performed by the Intermediary on:

(a) the IDA's main Public Wallet Addresses, and

(b) where applicable, the Public Wallet Addresses from which Digital Assets will be transferred to the Intermediary.

3. If the outcome of the Blockchain Forensic Analysis and/or the Wallet Ownership Verification is:

(a) satisfactory, then such Public Wallet Addresses are "white listed" and only transfers from such Public Wallet Addresses will be permitted by the Intermediary, unless additional Public Wallet Addresses are added at a later stage to the list of white listed addresses (after due completion of the same procedures); or

(b) not satisfactory, then the Intermediary shall take the necessary measures (e.g., additional clarifications, refusal of the business relationship with the IDA, reporting the relationship to the MROS).

4. If a non-negligible part of the source of wealth of the IDA stems from mining activities, the Intermediary shall apply specific enhanced due diligence measures depending on its risk-based approach. The information and documentation collected by the Intermediary should cover:

(a) total of the Fiat Currencies invested in mining material;

(b) origin of the Fiat Currencies used to acquire mining material;

(c) exact or at least approximate dates during which Digital Assets were mined;

(d) description of the Digital Assets mined by the IDA;

(e) total amount of Digital Assets mined by the IDA;

(f) description of the mining material acquired by the IDA to mine Digital Assets and relevant corroborative documentation (e.g., mining material order confirmations/receipts, pictures of the mining material, electricity bills);

(g) Wallet Ownership Verification on one or more Public Wallet Addresses which were credited with mining rewards, if applicable;

(h) list of the mining pools used to mine Digital Assets and relevant mining statements, if applicable; and

(i) confirmation of compliance with local tax rules in regards to the mining of Digital Assets as per the tax compliance policy of the Intermediary.

5. The decision of the Intermediary as regards the acceptance of a HRR shall be documented.

Section 3. Periodic review and update of the client file

1. The Intermediary shall perform a periodic review of client relationships. The frequency, scope and intensity of the review of the client relationship shall be determined on a risk-based approach, taking into account the nature of the business relationship with the IDA, as well as the specific risk profile of the IDA. By way of example, an Intermediary could choose to review the client relationship every two (2) years for normal risk relationships and every year for HRR.

2. The results of the review shall be documented.

3. In the event that any material changes are identified at any point in time including as a result of a periodic review of the client relationship, the Intermediary shall update the client file accordingly and take the appropriate measures.

CHAPTER 4. BUSINESS RELATIONSHIP WITH A MERCHANT

1. This chapter describes the standards that an Intermediary may decide to apply when examining a request to enter into a business relationship from a Merchant and when performing its monitoring activities after entering into the business relationship.

Section 1. General provisions

§ 1. Definition

1. For the purpose of this Chapter 4, "**Merchant**" shall mean a natural person or entity which:

(a) conducts a professional activity (business) which involves providing services or selling goods commercially; and

(b) accepts payments in Digital Assets from its customers totaling at least 10% of turnover or CHF 1 million per year as part of such business.

§ 2. Scope

1. The Standards set forth the due diligence procedures applicable to:

   (a) the onboarding of Merchants by an Intermediary; and

   (b) existing business relationships that, during the course of the business relationship, are identified by the Intermediary as Merchants, as part of the ongoing monitoring of relationships or during periodic reviews.

2. Such due diligence procedures are in addition to the applicable AML procedures to be performed by the Intermediary in application of, among others, AMLA, AMLO-FINMA, sanctions regimes and other applicable regulations.

§ 3. Excluded jurisdictions

1. For the purpose of this Chapter 4, an "**Excluded Jurisdiction**" shall mean a jurisdiction in which for legal, regulatory or other reasons the Merchant does not conduct its business and/or the Merchant has determined that payments from such Excluded Jurisdictions shall not be accepted.

2. The Merchant shall establish and keep up-to-date a list of Excluded Jurisdictions which shall take into consideration all sanctions or other restrictions applicable in Switzerland, as well as in each jurisdiction where the Merchant conducts its business.

Section 2. Inquiring on and verifying the source of revenues and wealth

§ 1. Generalities

1. The Merchant shall be required to complete a due diligence questionnaire (the "**DDQ-Merchant**"). The Intermediary may also complete the DDQ-Merchant on the basis of the information and documents provided by the Merchant.

2. The DDQ-Merchant shall cover the following information:

   (a) the types of services provided and/or goods sold, their jurisdiction of origin and the main providers;

   (b) the method of commercialization (e.g., own website or application, public platform, etc.);

   (c) the targeted markets (type of clients and countries) and Excluded Jurisdictions;

   (d) the global figures of the Merchant, including an estimation of the global volume of Digital Assets (in proportion to the activity in Fiat Currencies if applicable);

   (e) the Digital Assets accepted as means of payment;

   (f) information on the Merchant's sophistication, knowledge and background in relation to Digital Assets and/or DLT;

   (g) description of the Merchant's holdings of Digital Assets, together with the planned use of such holdings;

   (h) total current value of the Merchant's holdings of Digital Assets;

   (i) description and amount of the Digital Assets to be transferred to the Intermediary or in respect to which the Intermediary is to provide services, as applicable;

(j) list of the Merchant's main Public Wallet Addresses;

(k) list of the Public Wallet Addresses from which the Merchant intends to transfer Digital Assets to the Intermediary, if applicable;

(l) list of exchanges, brokers and platforms used by the Merchant to acquire, trade, sell and transfer Digital Assets and relevant account statements;

(m) confirmation of compliance with local tax rules in regards to Digital Assets as per the tax compliance policy of the Intermediary;

(n) confirmation that the Merchant will not receive on its account with the Intermediary Digital Assets from third parties and will not instruct the Intermediary to transfer Digital Assets to third parties (it being specified that transfers from or to Public Wallet Addresses owned by an exchange, a broker or another platform where the Merchant holds an account are not considered as third party transfers);

(o) description of the measures taken by the Merchant regarding the enforcement of AML requirements, if applicable; and

(p) confirmation that there is no link with Excluded Jurisdictions, whether in relation to the goods and services or the Merchant's clients.

3. An example DDQ-Merchant is enclosed as **Appendix D**.

4. Chapters 6 and 7 on Transaction Monitoring and Travel Rule respectively, apply in addition to this section in the case of Digital Asset transfers between a Merchant and the Intermediary.

§ 2. Enhanced due diligence

1. The Intermediary shall define, according to a risk-based approach, criteria (e.g., thresholds, business activity of Merchant, transaction patterns, etc.) on the basis of which the Intermediary will determine which business relationships with a Merchant should be classified as high risk relationships (HRR). Depending on its risk-based approach, an Intermediary may decide to treat all relationships with Merchants as HRR, regardless of the amounts involved and/or any other criteria.

2. A Blockchain Forensic Analysis shall be performed by the Intermediary on:

(a) the Merchant's main Public Wallet Addresses, and

(b) where applicable, the Public Wallet Addresses from which Digital Assets will be transferred to the Intermediary.

3. If the outcome of the Blockchain Forensic Analysis and/or the Wallet Ownership Verification is:

(a) satisfactory, such Public Wallet Addresses are "white listed" and only transfers from such Public Wallet Addresses will be permitted by the Intermediary, unless additional Public Wallet Addresses are added at a later stage to the list of white listed addresses (after due completion of the same procedures); or

(b) not satisfactory, the Intermediary shall take the necessary measures (e.g., additional clarifications, refusal of the business relationship with the Merchant, reporting the relationship to the MROS).

4. The decision of the Intermediary as regards the acceptance of a HRR shall be documented.

Section 3. Monitoring and update of the client file

1. The Intermediary shall perform a regular review of the client relationships. The frequency and intensity of the review of the client relationship shall be determined on a risk-based approach, taking into account the nature of the business relationship with the Merchant, as well as the specific risk profile of the Merchant. By way of example, an Intermediary could choose to review the client relationship every two (2) years for normal risk relationships and every year for HRR.
2. The results of the review shall be documented.
3. In the event that any material changes are identified at any point in time including as a result of a regular review of the client relationship, the Intermediary shall update the client file accordingly and take the appropriate measures.

CHAPTER 5. BUSINESS RELATIONSHIP WITH A VIRTUAL ASSET SERVICE PROVIDER (VASP)

Section 1. General provisions

§ 1. Definition

1. For the purpose of this Chapter 5, "**VASP**" shall mean a natural person or entity which as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
   (a) exchange between Digital Assets and fiat currencies;
   (b) exchange between one or more forms of Digital Assets;
   (c) transfer of Digital Assets;
   (d) safekeeping and/or administration of Digital Assets or instruments enabling control over Digital Assets; and/or
   (e) participation in and provision of financial services related to an Issuer's Offering and/or sale of Digital Assets.

§ 2. Scope

1. The Standards set forth the due diligence procedures applicable to:
   (a) the onboarding of VASPs by an Intermediary; and
   (b) existing business relationships that, during the course of the business relationship, are identified by the Intermediary as a VASP, as part of the ongoing monitoring of relationships or during periodic reviews.
2. Such due diligence procedures are in addition to the applicable AML procedures to be performed by the Intermediary in application of, among others, AMLA, AMLO-FINMA, sanctions regimes and other applicable regulations.

§ 3. Excluded jurisdictions

1. For the purpose of this Chapter 5, an "**Excluded Jurisdiction**" shall mean a jurisdiction in which for legal, regulatory or other reasons the VASP does not conduct its business and/or the VASP has determined that payments or transfers to or from such Excluded Jurisdictions shall not be accepted.
2. The VASP shall establish and keep up-to-date a list of Excluded Jurisdictions which shall take into consideration all

sanctions or other restrictions applicable in Switzerland, as well as in each jurisdiction where the VASP conducts its business.

Section 2. Know Your VASP (KYVASP)

§ 1. Collection of relevant information

1. The VASP shall be required to provide additional information and documentation to allow the Intermediary to perform its risk-based assessment. The Intermediary may collect additional information and documentation on the VASP through its own independent due diligence and research, rather than requesting it from the VASP.

2. At a minimum, the following information and documentation should be covered, which shall be used to define the risk profile of the VASP and inform the selection of further due diligence measures, defined on a risk-based approach by the Intermediary:

   (a) the VASP's jurisdiction;

   (b) the VASP's regulatory status in the jurisdiction it operates in;

   (c) the VASP's business model (services), targeted markets and current clientele (countries, PEP, etc.);

   (d) the VASP's organization (group, company, compliance);

   (e) the VASP's AML organization, AML policy, etc.;

   (f) the VASP's control framework in terms of AML compliance (e.g., inspection from the regulator, external audit, etc.); and

   (g) the information relevant to assess the VASP's reputation (e.g., litigation, regulatory action or sanctions).

3. Depending on the preliminary assessment of the initial information and the purpose of the business relationship with the VASP, the following further due diligence measures should be considered by the Intermediary:

   (a) review and document the business model of the VASP, its regulatory status in the relevant jurisdictions, as well as the extent and scope of the prudential supervision to which such VASP is subject, if any (e.g., research, public documents, official registers of licensed entities, legal opinions, etc.);

   (b) perform in-depth independent research regarding the prospective VASP and, to the extent relevant, the VASP's key persons (e.g., World-Check or WorldCompliance, online research (e.g., Google) and breaches indicated in the register of the relevant authority, if any);

   (c) review the privacy attributes of Digital Assets offered for transfers to the VASP's clientele;

   (d) analyze the software, tools and methods (incl. parameters, thresholds, etc.) used by the VASP to perform a Blockchain Forensic Analysis;

   (e) if considered appropriate by the Intermediary, discuss with the VASP's Compliance Officer/MLRO; and

   (f) exceptionally, perform an on-site visit with the VASP by the representatives of the Intermediary.

§ 2. Identification of the VASP as Contracting Party

1. The verification of the identity of the VASP as the Intermediary's "**Contracting Party**" shall be performed in accordance with the AML requirements applicable to the Intermediary (e.g., CDB, SRO Regulations, and/or AMLO-FINMA). The

same shall apply to the establishment of the identity of the controlling person(s) and the establishment of the identity of the beneficial owner(s) of the assets.

Section 3. Assessment and acceptance of business relationship

§ 1. Assessment of the information obtained

1. The Intermediary shall carefully review the information obtained and assess the level of due diligence requirements of the VASP against the AML requirements for VASPs which are subject to AML regulations in their jurisdiction and/or Switzerland.

2. The Intermediary shall document the findings of the assessment, with explanations or comments for material discrepancies or derogations to the applicable minimum level of expected due diligence, in accordance with its risk-based approach policy.

§ 2. Acceptance of business relationship

1. Based on the outcome of the assessment and the risk appetite of the Intermediary, the Intermediary shall decide whether it approves the business relationship with the VASP depending on its risk-based approach.

2. The Intermediary shall establish criteria on the basis of which the Intermediary will determine which business relationships with a VASP are to be classified as high risk relationships (HRR). Depending on its risk-based approach, an Intermediary may decide to treat all relationships with VASPs as HRR, regardless of the purpose of the business relationship, of the amounts concerned or any other criteria.

3. In case of doubt as to the risk classification, a relationship with a VASP should be considered as HRR, given the increased operational, legal and reputational risks involved in such a relationship.

4. The decision of the Intermediary as regards the acceptance of a HRR shall be documented.

Section 4. Monitoring and update of the client file

1. The Intermediary shall perform a regular review of the client relationships. The frequency and intensity of the review of the client relationship shall be determined on a risk-based approach, taking into account the nature of the business relationship with the VASP, as well as the specific risk profile of the VASP. By way of example, an Intermediary could choose to review the client relationship every two (2) years for normal risk relationships and every year for HRR.

2. The results of the review shall be documented.

3. In the event that any material changes are identified at any point in time including as a result of a regular review of the client relationship, the Intermediary shall update the client file accordingly and take the appropriate measures.

CHAPTER 6. TRANSACTION MONITORING

Section 1. General principles

§ 1. Policies and procedures

1. The Intermediary shall define policies and procedures, on a risk-based approach, designed to monitor:

(a) normal risk Digital Asset transactions ("**NRT**"); and

(b) high risk Digital Asset transactions ("**HRT**").

2. A Wallet Ownership Verification must be carried out before the relevant incoming or outgoing transfer of Digital Assets or at least prior to crediting any Digital Assets to the client account, and the steps and results of the Wallet Ownership Verification must be adequately documented.

3. In case of doubt with respect to the control of the private key corresponding to the relevant Public Wallet Addresses or where the Intermediary deems it required or appropriate, the Intermediary:

(a) clarifies the situation with the client by means of written or oral explanations alongside corroborative documentation (e.g., screenshots); and/or

(b) depending on the circumstances, obtains additional Wallet Ownership Verification or enhanced live Wallet Ownership Verification (e.g., via video-conference with the client or by phone).

4. If the client did not pass the Wallet Ownership Verification, the Intermediary shall take appropriate measures depending on the circumstances, including, as applicable, instructing the return of the Digital Assets (if already received), carrying out additional due diligence, terminating or declining to enter into a business relationship with the client and/or reporting the case to the MROS.

§ 2. Additional requirements - Transfers to or from a VASP

1. By way of exception to § 1, for a transfer of Digital Assets to or from a Public Wallet Address controlled by a VASP vetted by the Intermediary, i.e., reviewed and considered an acceptable service provider by the Intermediary (the "**Vetted VASP**"), so that the client has no control over the private keys relating to such Public Wallet Addresses, the Intermediary may obtain from the client the relevant account/wallet documentation (e.g., screenshot of the client's account interface) which demonstrates to the satisfaction of the Intermediary that the client indeed holds such account/wallet with the stated VASP.

2. The Intermediary shall put in place an approval procedure and regular reviews of Vetted VASPs. As part of the approval procedure, the Intermediary assesses *inter alia* the corporate as well as ownership structure, business model, regulatory status and AML & KYC procedures of the respective VASP. The Intermediary can define additional criteria that need to be assessed as part of the approval procedure.

3. The clarifications performed before the relevant incoming or outgoing transfer of Digital Assets, and the results of such clarifications, must be adequately documented.

4. For the purposes of this Section, the following categories of VASPs are eligible to be considered as a Vetted VASP by the Intermediary:

(a) any Swiss Intermediary as defined in Article 2 §2 AMLA;

(b) any foreign Intermediary or VASP which has its registered office or domicile in a foreign jurisdiction which is subject to an appropriate prudential supervision and AML regulation; and

(c) any other Swiss or foreign VASP which the Intermediary has determined to be subject to appropriate AML regulation in its jurisdiction, even without any prudential supervision over the VASP services relating to Digital Assets (each such non-prudentially supervised VASP, a "**NPS-VASP**").

Section 2. NRT

§ 1. Definition and principles

1. Digital Asset transactions that do not constitute HRT are considered NRT.

2. The Intermediary shall apply at least the same monitoring policies and procedures to NRT in Digital Assets as to any other normal risk transactions.

§ 2. Additional procedures

1. In addition to ordinary monitoring steps, the Intermediary shall implement a screening of NRT via tools for a Blockchain Forensic Analysis. In case the screening results are that one or several risk indicators are identified above a materiality threshold defined by the Intermediary on a risk-based approach, the Intermediary must implement an approval process for the NRT.

2. As part of the approval process, the Intermediary shall:

   (a) obtain an enhanced report from the same or a different Blockchain Forensic Analysis provider; and/or

   (b) undertake additional clarifications depending on the circumstances, which may include some or all of the clarifications applicable to HRT.

Section 3. HRT

§ 1. Definition

1. Digital Asset transactions are considered as HRT:

   (a) by applying an automated IT screening based on certain high risk criteria ("**HRC**"), or

   (b) based on a determination by the Intermediary based on review of HRC or other criteria; and/or

   (c) if the transactions otherwise qualify as high risk transactions under AMLA, AMLO-FINMA or the Intermediary's AML policies and procedures, applicable to all transactions generally.

2. The Intermediary shall determine the HRC which are appropriate to the Intermediary's business model, type of clients and services offered. An example of a risk-based approach for HRC relating to Digital Asset transactions is enclosed as **Appendix E**.

3. In addition to the indicia of money laundering pursuant to the Annex to the AMLO-FINMA, the Intermediary should also consider criteria specific to Digital Assets in accordance with its risk-based approach. Examples of such specific criteria are added below:

   (a) Digital Assets transferred from/to a Public Wallet Address with direct or indirect exposure links to known suspicious sources, including darknet marketplaces, mixing services, questionable gambling sites, illegal activities (e.g., ransomware) and/or theft reports;

   (b) the Digital Assets transferred from/to a Public Wallet Address are connected to an exchange, broker or platforms which have been connected to money laundering, or which law enforcement has shut down;

   (c) abnormal transactional activity (level and volume) of Digital Assets on peer-to-peer platforms; or

   (d) use of Digital Assets whose design is not adequately documented, or that are linked to possible fraud or other

tools aimed at implementing fraudulent schemes, such as Ponzi schemes.

4. A single indicia or criteria may not in itself give sufficient grounds for suspecting money laundering, terrorist financing or other relevant misbehaviours, and some indicia are only relevant when in combination with other factors. The Intermediary shall define on a risk-based approach the manner in which indicia and HRC will be captured and processed.

§ 2. Applicable procedures

1. HRT are subject to additional clarifications by the Intermediary as soon as possible.

2. Depending on the circumstances, clarifications may include:

   (a) whether the client is the beneficial owner of the Digital Assets;

   (b) the origin of the deposited Digital Assets;

   (c) the planned use of the Digital Assets;

   (d) the economic background of significant incoming Digital Assets deposits and their plausibility;

   (e) the origin of the wealth of the client and/or beneficial owner and/or controlling person;

   (f) the professional or commercial activity of the client and/or beneficial owner and/or controlling person;

   (g) whether the client, beneficial owner, controlling person and/or holder of a power of attorney is a PEP;

   (h) information in written or oral form from the client, beneficial owner, controlling person, holder of a power of attorney, independent asset manager and/or introducing broker;

   (i) visits to the premises where the client, beneficial owner and/or controlling person conducts business;

   (j) sources and databases available to the Intermediary; or

   (k) information from trustworthy persons.

   The Intermediary may also commission an enhanced report via a Blockchain Forensic Analysis provider.

3. In any event, the Intermediary shall review and assess the identified HRT and the corresponding explanations, so as to verify the plausibility of the results of these clarifications and, to the extent possible and appropriate, obtain independent evidence to corroborate such results.

4. The clarifications conducted and the results of their analysis and assessment shall be documented.

5. Based on the results of the clarifications performed, the Intermediary takes appropriate measures, including, as applicable, instructing the transfer of the Digital Assets, requesting an (additional) external due diligence report, terminating the relevant relationship or reporting the case to the MROS.

CHAPTER 7. TRAVEL RULE IMPLEMENTATION

Section 1. General principles

§ 1. Definition

1. A Digital Asset transfer between an Intermediary and a VASP ("**VASP-to-VASP transfer**") refers to any operation where an Intermediary (the "**Originating VASP**") transfers Digital Assets on behalf of an originating party with a view to making them available to a beneficiary party (which may be the originating party itself) at (or through) a VASP (the "**Beneficiary VASP**"). The originating party and the beneficiary party are referred to together as "**Contracting Party**" or "**Contracting Parties**".

2. When performing a VASP-to-VASP transfer, Intermediaries shall apply the Travel Rule (i.e., exchange of information, as defined in §2, between the VASPs).

Section 2. Travel Rule

§ 1. Principle

1. For every VASP-to-VASP transfer, the Originating VASP must ensure the following information is communicated to the Beneficiary VASP prior to or simultaneously with the transfer of Digital Assets:

   (a) Name of the originating party;

   (b) Account number of the originating party, or, if not available, the transaction reference number;

   (c) Postal address, or, if not available the place and date of birth, client number, or national ID number of the originating party;

   (d) Name of the beneficiary party; and

   (e) Account number of the beneficiary party, or, if not available, the transaction reference number.

2. Transfer of Digital Assets is permissible without exchanging the above-mentioned information, if the originating party and the beneficiary party are Contracting Parties in case of internal transfers within the same VASP.

3. For VASP-to-VASP transfers within Switzerland, Intermediaries may restrict themselves to providing the account number or a transaction-based reference number of the originating party and the beneficiary party, provided they are able to provide the remaining information on the Contracting Parties to the Beneficiary VASP and/or to the competent Swiss authorities within three (3) working days of a request.

§ 2. Acceptable means of communication

1. The information mentioned in §1 above:

   (a) must be transferred in the form of a text;

   (b) can be transferred by any appropriate means of communication, including:

      (1) Email;

      (2) Dedicated Travel Rule message protocols; or

(3) Metadata to the Digital Assets transfer (or other similar on-chain mechanism).

§ 3. Choice of the means of communication

1. In choosing the appropriate means of communication, Intermediaries should adopt a pragmatic approach, and may use whichever means of communication is most practicable at the time of the VASP-to-VASP transfer, to the extent that the applicable law or regulations, including guidance of the competent authorities does not impose a specific means of communication[1].

§ 4. Transfer to self

1. If (i) the Contracting Party is both the originating party and the beneficiary party of the VASP-to-VASP transfer (i.e., transfer to self), (ii) the VASP-to-VASP transfer is originated by the Contracting Party at or through the Originating VASP and (iii) the VASP-to-VASP transfer is received by the Contracting Party at or through the Beneficiary VASP, then the Originating VASP and the Beneficiary VASP must exchange the Travel Rule information in accordance with §1 above.

§ 5. Incoming transfers with incomplete or inconsistent information

1. If a Beneficiary VASP receives a VASP-to-VASP transfer that does not comply with the above requirements, the Beneficiary VASP must determine the appropriate process and response, according to a risk-based approach. The Beneficiary VASP may, for example:

   (a) request complementary information from the Originating VASP or conduct further investigations as it may deem appropriate;

   (b) request additional information from the beneficiary party;

   (c) return the Digital Assets to the Originating VASP in favor of the originating party after clarification of the correct return address and/or coordinating with the Originating VASP; and/or

   (d) close the relevant account or report the case to the MROS, if it has reasonable suspicion of money laundering and terrorist financing as set out in AMLA.

CHAPTER 8. TRANSFERS TO AND/OR FROM SELF-HOSTED WALLETS

Section 1. General provisions

§ 1. Definitions

1. For the purposes of this clause:

   (a) Self-Hosted Wallet means a distributed ledger address controlled by a person or an entity that is not a VASP.

   (b) VASP Client refers to any person or entity who maintains a business relationship or account with the respective VASP.

   (c) Third Party refers to any person or entity who does not maintain a business relationship or account with the respective VASP.

1 At the time of writing, no specific means of communication are imposed by the AMLA, by FINMA or by an SRO.

Section 2. Transfers

§ 1. Transfers to/from a Self-Hosted Wallet belonging to a VASP Client

1. If a VASP receives or initiates a transfer of Digital Assets to/from a Self-Hosted Wallet belonging to a VASP Client, the Intermediary shall perform a Wallet Ownership Verification on such Self-Hosted Wallet.

§ 2. Transfer to/from a Self-Hosted Wallet belonging to a Third Party

1. If a VASP receives or initiates a transfer of Digital Assets to/from a Self-Hosted Wallet belonging to a Third Party, the Intermediary must:

   (a) verify the identity of the Third Party in accordance with AMLA, as if the Intermediary were to enter into a business relationship with such Third Party;

   (b) establish the identity of the beneficial owner of the Self-Hosted Wallet; and

   (c) perform a Wallet Ownership Verification on the Self-Hosted Wallet to ensure that the Third Party identified by the Intermediary is effectively the owner of the Self-Hosted Wallet.

APPENDIX A GLOSSARY

Defined term	Definition
AML	Anti-Money Laundering.
AMLA	Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act; RS 955.0).
AMLO	Anti-Money Laundering Ordinance (RS 955.01).
AMLO-FINMA	FINMA Anti-Money Laundering Ordinance (RS 955.033.0).
Asset Tokens	See Token.
Blockchain Forensic Analysis	Review of the transactions performed on a specific Public Wallet Address in relation to one or more Public Wallet Addresses with the purpose of, in particular, determining to the extent possible whether: • such Public Wallet Addresses are known to be associated with illegal transactions or other Public Wallet Addresses that are thought to be used for illegal purposes; • such Public Wallet Addresses are known to be associated with money laundering, financing of terrorism or cybercrime (e.g., stolen Digital Assets); • such Public Wallet Addresses are known to be associated with transactions on the Dark Web; • transactions relating to such Public Wallet Addresses are not (or less) traceable due to darkening/obscuring techniques (e.g., mixing, conjoining, u-turn transactions); • such Public Wallet Addresses are known to be associated with miners or other entities and are therefore, as a result of the business activities of such miners or other entities, not (or less) traceable; and/or • such Public Wallet Addresses are known to be associated with transactions relating to sanctioned countries or persons, respectively persons identified as enabling circumvention of sanctions. A Blockchain Forensic Analysis requires an appropriate clustering of Public Wallet Addresses by appropriate technical means. The Blockchain Forensic Analysis shall take into account the specificities of the respective DL protocol.
CDB	Current version of the "Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence", as issued by the Swiss Bankers Association.
CFT	Countering the financing of terrorism.
Contracting Party	Person or entity entering into a business relationship with an Intermediary.
Contribution Amount	Contributor's contemplated contribution in an Offering.
Contributor	Any person or entity participating in an Offering.

Defined term	Definition
Cryptocurrencies	Cryptocurrencies are a subset of Digital Assets that rely on cryptographic techniques to achieve consensus (e.g., Bitcoin and ether). See also Payment Token.
DDQ	Due Diligence Questionnaire
Dark Web	Encrypted online content that is not indexed on conventional search engines. The Dark Web is part of the deep web that does not appear through regular internet browsing.
Digital Assets	Any type of financial assets, whether natively digital or digitised, issued through the use of DLT such as Payment Tokens, Utility Tokens and Asset Tokens. See also Token.
Distributed Ledger (DL)	Database that is consensually shared and synchronized according to a protocol by nodes participating in a peer-to-peer decentralized network. It allows transactions to have public "witnesses" who can access the recordings shared across that network and can each store an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all nodes. One form of distributed ledger design is the blockchain, which can be either public, permissioned or private.
Distributed Ledger Technology (DLT)	Technology recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants.
Excluded jurisdiction	Jurisdiction in which for legal, regulatory or other reasons, depending on context: • an Offering is not permitted to be conducted and/or the Issuer has determined that contributions from such excluded juris-dictions shall not be accepted; • the Merchant does not conduct its business and/or the Mer-chant has determined that payments received from such ex-cluded jurisdictions shall not be accepted; or • a VASP does not conduct its business and/or the VASP has determined that incoming payments or transfers from such Excluded Jurisdictions shall not be accepted.
Fiat Currency	Currency designated by applicable law as legal tender in the relevant jurisdiction, such as national currencies in circulation, issued and managed by the respective central banks.
HRC	High risk criteria
HRR	High risk relationship
IDA	Investor in Digital Assets
Intermediary	Swiss bank, securities firm or other financial intermediary pursuant to Article 2 §2 or §3 AMLA.
Initial Coin Offering (ICO)	Method of raising funds by issuing Digital Assets in exchange for Cryptocurrencies and/or Fiat Currencies.

Defined term	Definition
Issuer	Person or entity issuing and offering Digital Assets.
Merchant	Natural person or entity which: • conducts a professional activity (business) which involves providing services or selling goods; and • accepts payments in Digital Assets from its customers totalling at least 10% of turnover or CHF 1 million per year as part of such business.
MROS	Money Laundering Reporting Office Switzerland (https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/geldwaescherei.html).
NPS-VASP	Any Swiss or foreign VASP which the Intermediary has determined to be subject to appropriate AML regulation in its jurisdiction, even without any prudential supervision over the VASP services relating to Digital Assets.
Offering	The issuance or offering of Digital Assets.
Payment Token	See Token.
Public Wallet Address	A unique alphanumeric string generated through cryptographic algorithms that serves as an identifier for a specific DL wallet and is unique to each wallet. It is publicly accessible and used by others to transfer digital assets to that particular wallet.
Standards	CMTA's Digital Assets - AML Standards for Financial Intermediaries.
Token	Digital Asset which may have various features, depending on the DLT on which it was issued and the terms of the issuance. The primary types of Tokens, as per the Swiss Financial Markets Supervisory Authority FINMA's classification: • **Payment Tokens** are generally synonymous with Cryptocurrencies, the sole or primary purpose and function of which is to serve as a means of payment, so that Payment Tokens have no other material functions or links to development projects. • **Utility Tokens** are Digital Assets that are intended to provide digital access to an application or service. • **Asset Tokens** represent assets such as participations in real physical underlyings, companies, or earnings streams, or an entitlement to dividends or interest payments. In terms of their economic function, Asset Tokens are analogous to equities, bonds, derivatives or other investment instruments. In many instances, Tokens will be a hybrid combination of the above primary types, depending on their features.
Utility Token	See Token.
VASP (Virtual Asset Service Provider)	A natural person or entity which conducts activities or operations for or on behalf of another natural or legal person and meets the following criteria: • provision of financial services relating to Digital Assets that entail non-negligible AML/CTF risks (e.g., transfers of Digital Assets); and • the extent of Digital Assets-related revenues or any other factor do not make it inappropriate or irrelevant to consider the natural person or entity a “VASP”.

Defined term	Definition
Vetted VASP	• A VASP that has been vetted by the Intermediary.
Wallet Ownership Verification Methods (Wallet Ownership Verification)	Procedures aiming at ascertaining that the private key corresponding to the Public Wallet Address is controlled by the relevant person, which is an indication that such relevant person may be the legal and economic owner of such Public Wallet Address. Each of the following procedures are examples of Wallet Ownership Verification Methods: • the relevant person transfers a small amount of Digital Assets designated by the Intermediary from the person's own Public Wallet Address to a Public Wallet Address designated by the Intermediary within a specified time period (so-called "satoshi test"); • the relevant person gives to the Intermediary prior notice of the transaction and the desired amount to be transferred to the Intermediary, whereupon the Intermediary will notify a Public Wallet Address available only to the relevant person, for the purpose of effecting the transaction within a specified time period; • the relevant person signs a specific message from the person's own Public Wallet Address within a specified time period; • the relevant person unlocks (i.e., is able to sign a transaction on) the Public Wallet Address with the corresponding private key in the presence of the Intermediary or the Intermediary's agent (e.g., service provider).

APPENDIX B EXAMPLE OF DDQ-ISSUER

Preliminary note:

This questionnaire was drafted to take into consideration a planned Token Offering. If the Token Offering already took place, the questions of this questionnaire remain valid: please answer accordingly.

1. ISSUER AND OTHER RELEVANT MATERIAL ENTITIES

1.1 Name	
1.2 Full address	
1.3 Type of legal entity	
1.4 Commercial register number	
1.5 Website	
1.6 Organization chart of the Issuer	
1.7 Organization chart of the group of the Issuer	
1.8 Copy of latest financial statements	
1.9 Regulatory status	

In case the Issuer is not the legal entity developing the business plan referred to in Section 4, please also provide the same details in respect of that legal entity.

2. DIRECTORS, MANAGEMENT & KEY PERSONNEL

2.1 Personal details (Issuer):	For each of the members of the board of directors, senior management and/or other key persons: 2.1.1 First name 2.1.2 Last name 2.1.3 Full address 2.1.4 Date of birth 2.1.5 Short biography Alternative: CV of each of these persons

In case the Issuer is not the legal entity developing the business plan referred to in Section 4, please also provide the same details in respect of that legal entity:

2.2 Personal details (relevant material entity)	For each of the members of the board of directors, senior management and/or other key persons: 2.2.1 First name 2.2.2 Last name 2.2.3 Full address 2.2.4 Date of birth 2.2.5 Short biography Alternative: CV of each of these persons

3. MAJOR SHAREHOLDERS

Note: any person or entity holding 10% or more of the shares of the Issuer or of the voting rights is a major shareholder for the purposes of this questionnaire.

3.1 Personal details (major shareholders of Issuer)	For each of the members of the board of directors, senior management and/or other key persons: 3.1.1 First name 3.1.2 Last name 3.1.3 Full address 3.1.4 Date of birth 3.1.5 Short biography Alternative: CV of each of these persons

In case the Issuer is not the legal entity developing the business plan referred to in Section 4, please also provide the same details in respect of that legal entity:

3.2 Personal details (major shareholders of relevant material entity)	For each of the members of the board of directors, senior management and/or other key persons: 3.2.1 First name 3.2.2 Last name 3.2.3 Full address 3.2.4 Date of birth 3.2.5 Short biography Alternative: CV of each of these persons

4. BUSINESS PLAN

4.1 Short description of the business plan, including information on the key milestones	
4.2 Information on the technologies to be used (incl. indication whether the business plan relies on open source software and/or will lead to the development of open source software)	
4.3 Connection between the business plan and Distributed Ledger Technologies (if any; e.g., decentralization of a centralized service) and, in this context, role played by the Token offered	
4.4 Copy of full business plan, white paper, brochures and other documents describing the products and/or services offered by the Issuer	

4.5 Description of the main business risks/challenges relating to the business plan	4.5.1 market 4.5.2 competition 4.5.3 financing 4.5.4 regulation 4.5.5 IT systems 4.5.6 time-to-market 4.5.7 human resources 4.5.8 other risks
4.6 Description of the Issuer's competitive advantage	
4.7 Copy of any research paper backing the Issuer's business plan	
4.8 Key one-year projections in terms of:	4.8.1 headcount 4.8.2 revenues 4.8.3 pre-tax profit 4.8.4 capex 4.8.5 equity 4.8.6 debt 4.8.7 cash flow 4.8.8 net cash position 4.8.9 market share

4.9 Key five-year projections in terms of:	4.9.1 headcount 4.9.2 revenues 4.9.3 pre-tax profit 4.9.4 capex 4.9.5 equity 4.9.6 debt 4.9.7 cash flow 4.9.8 net cash position 4.9.9 market share

5. TOKEN OFFERING

5.1 Reasons for the Issuer to launch a Token Offering	
5.2 Timing of the pre-sale(s), the public Offering and the subsequent steps/milestones of development of the business plan (road map)	
5.3 Targeted amount (with a distribution between pre-sale(s) and public Offering) and underlying reasons	
5.4 Amount of Tokens to be offered and underlying reasons	
5.5 Soft cap and hard cap and underlying reasons	
5.6 List of Cryptocurrencies and Fiat Currencies accepted during the Offering	
5.7 Information on the Tokens reserved for the members of the board of directors, the senior management, the employees and other persons involved in the business plan and/or the Offering (e.g., advisors)	

5.8 Description of the targeted Contributors	
5.9 Description of the restrictions applicable to Contributors (e.g., prohibited countries)	
5.10 Description of the regime of discount or bonus and underlying reasons	
5.11 Description of the material to be produced for the Offering and indication on the languages used in such material	
5.12 Description of planned roadshows (if any)	
5.13 Description of online marketing (e.g., webinar, Reddit AMA)	
5.14 Description of the opportunity for the Contributors	
5.15 Description of the main risks incurred by Contributors (e.g., business, market, liquidity risks)	
5.16 Description of the worst case scenario for the Contributors	
5.17 Information on the subscription and redemption processes, including on any optional or mandatory buy back process (i.e., forced redemption)	
5.18 Information on when the Token will be transferred to the Contributors	
5.19 Information on what will be done with unsold Tokens	
5.20 Information on how surplus funds (if any) will be handled/allocated	
5.21 Level of confidence of the senior management with respect to the achievement of the targeted amount	

6. TOKEN FEATURES

6.1 Name and symbol	
6.2 Underlying platform (e.g., Ethereum, NEO)	
6.3 Consensus algorithm used and reasons for this choice (if not resulting from the choice of the underlying platform)	
6.4 So-called "fiscal policy" (e.g., instamines, premines, buying, spending, icing, discounting, or burning of Tokens)	
6.5 So-called "monetary policy" (e.g., inflationary, deflationary, fixed supply or additional Tokens to be issued)	
6.6 Estimate of the time required by the network to launch and adopt the Token	
6.7 Price setting mechanism	
6.8 Rights/functionalities included in the Token, together with an estimate of the timing and information on how such rights/functionalities are documented (e.g., participation and issuing conditions)	
6.9 Indication whether the above-mentioned rights/functionalities are already usable	
6.10 Information whether the Token can be used to buy goods or services or make payments to third parties	
6.11 Information on wallets compatible with the Token, together with relevant technical specifications	
6.12 Information on any potential listing on a crypto-exchange	

7. LEGAL AND REGULATORY SITUATION

7.1 Copy of any legal opinion obtained from a law firm	
7.2 Copy of any tax opinion and tax ruling (e.g., VAT)	
7.3 Copy of any intellectual property opinion	
7.4 Copy of FINMA's ruling (if any)	
7.5 If not covered by the previous items, detailed explanations on the qualification of the Token and its legal and regulatory consequences (e.g., securities laws, money laundering laws)	
7.6 Specific information on the application of U.S. laws and/or regulations to the Token Offering (e.g., SEC regulations)	
7.7 Information on current and past (in the last 5 years) claims and litigations encountered by the Issuer or any related legal entities or private persons in relation to the business plan	

8. ADVISORS AND OTHER PERSONS INVOLVED IN THE BUSINESS PLAN AND/OR THE OFFERING

8.1 Details on the law firm mandated by the Issuer	
8.2 Details on the tax advisor mandated by the Issuer	
8.3 Details on the auditors mandated by the Issuer	
8.4 Details on any Swiss Intermediary subject to Swiss money laundering laws mandated by the Issuer to meet the due diligence requirements under Swiss AML laws	

8.5 Details on any Token sellers, ICO organizers, etc. (incl. on their regulatory status such as licenses under financial markets law)	
8.6 Details on the intellectual property expert mandated by the Issuer	
8.7 Details on any early backers	
8.8 Details on any person having an influence on the business plan and/or the Offering and who is a related party to the Issuer's or the legal entity's member of the board of directors, member of the senior management or share-holders	
8.9 Details on other key persons involved in the business plan and/or the Offering	

9. INTELLECTUAL PROPERTY

9.1 List of intellectual property material owned or licensed that are mandatory or important for the realization of the business plan	
9.2 For each intellectual property material licensed, details of the owner, start of the license, description of the most relevant rights and obligations under the license, end date (if any)	

10. FIGHT AGAINST MONEY LAUNDERING (AML) AND TERRORISM FINANCING (CFT)

10.1 Description of the general approach (due diligence Tiers, etc.)	

10.2 If the proposed due diligence measures are covered, please tick the appropriate box and provide any relevant information in the empty space.	☐ Check of an identification document _____ ☐ Check of a selfie against the photograph on the identification document _____ ☐ Check address against Excluded Jurisdictions _____ ☐ Check against sanctions, politically exposed persons and adverse media databases _____ ☐ Check of the phone number _____ ☐ Blockchain Forensic Analysis of the Public Wallet Address from which funds will be transferred _____ ☐ Prevention or handling of multiple participations by the same Contributor _____ ☐ Check of the IP address _____ ☐ Check of a proof of residence (e.g., utility bill) _____ ☐ Check of the source of the funds _____ ☐ Check of the source of wealth _____ ☐ Video-conference

10.3 Information on any mandated service provider in the field of AML/CFT	

11. VARIOUS

11.1 Measures to prevent scammers from misleading Contributors into sending funds to an incorrect address	
11.2 Other cybersecurity measures put in place/used	
11.3 Information on the cold storage solution used for storing the Cryptocurrencies accepted as investment and the Tokens offered	

APPENDIX C EXAMPLE OF DDQ-IDA

Applicable to business relationships with IDAs (in addition to standard AML procedures of the Intermediary).

1. BACKGROUND AND KNOWLEDGE

1.1 Description of the IDA's background in relation to Digital Assets and/or DLT (e.g., previous or current occupation, studies)	
1.2 In general, description of the IDA's knowledge and expertise in relation to Digital Assets and/or DLT	

2. INVESTMENTS IN DIGITAL ASSETS

2.1 Total and origin of the Fiat Currencies the IDA invested in Digital Assets	
2.2 Date of the IDA's first investment(s) in Digital Assets	
2.3 Description of the IDA's current holdings of Digital Assets	
2.4 Total current value of the IDA's current holdings of Digital Assets	
2.5 Planned use of the IDA's current holdings of Digital Assets (e.g., long term investments, payment for services)	
2.6 Description and amount of the Digital Assets to be transferred to the Intermediary or in respect to which the Intermediary is to provide services, as applicable	

2.7 List of exchanges, brokers and platforms used by the IDA to acquire, trade, sell and transfer Digital Assets, together with a copy of the relevant account statements	
2.8 Description of past uses of Digital Assets	
2.9 Please confirm that the IDA complies with local tax rules in regards to Digital Assets	

3. PUBLIC WALLET ADDRESSES

3.1 List of the IDA's main Public Wallet Addresses	Alternative: provide respective QR Codes (if more convenient)
3.2 List of the Public Wallet Addresses from which the IDA intends to transfer Digital Assets to the Intermediary, if applicable	Alternative: provide respective QR Codes (if more convenient)

APPENDIX D EXAMPLE OF DDQ-MERCHANT

1. MERCHANT'S BUSINESS ACTIVITIES

1.1 Services provided and/or goods sold by the Merchant	
1.2 Main providers of the goods sold by the Merchant (where applicable), incl. countries of origin	
1.3 Method of commercialisation (own website or application, public platform, etc.)	
1.4 Marketing (promotion) means	
1.5 Targeted clients	
1.6 Targeted countries and Excluded Jurisdictions	

2. USE OF DIGITAL ASSETS BY THE MERCHANT

2.1 Digital Assets accepted as a means of payment	
2.2 Global figures of the Merchant, including an estimation of the global volume of Digital Assets (in proportion to the activity in Fiat Currencies if applicable)	
2.3 List of the Merchant's main Public Wallet Addresses on which it receives Digital Assets	Alternative: provide respective QR Codes (if more convenient)
2.4 Description of the Merchant's holdings of Digital Assets, together with the planned use of such holdings	
2.5 Total current value of the Merchant's holdings of Digital Assets	

2.6 Description and amount of the Digital Assets to be transferred to the Intermediary or in respect to which the Intermediary is to provide services, as applicable	
2.7 List of the Public Wallet Addresses from which the Merchant intends to transfer Digital Assets to the Intermediary, if applicable	Alternative: provide respective QR Codes (if more convenient)
2.8 List of exchanges, brokers and platforms used by the Merchant to acquire, trade, sell and transfer Digital Assets and relevant account statements	
2.9 Past uses of Digital Assets	
2.10 Please confirm that the Merchant will not receive on its account with the Intermediary Digital Assets from third parties and will not instruct the Intermediary to transfer Digital Assets to third parties (it being specified that transfers from or to Public Wallet Addresses owned by an exchange, a broker or another platform where the Merchant holds an account are not considered as third party transfers)	

3. ORGANISATION OF THE MERCHANT IN RELATION TO DIGITAL ASSETS

3.1 Information on the Merchant's sophistication, knowledge and background in relation to Digital Assets and/or DLT	
3.2 Legal or regulatory clarifications carried out in relation to the use of Digital Assets in the Merchant's business, if applicable	
3.3 Description of the measures taken by the Merchant regarding the enforcement of AML requirements, if applicable	

3.4 Please confirm that there is no link with Excluded Jurisdictions, whether in relation to the goods and services or the Merchant's clients	
3.5 Please confirm that the Merchant complies with local tax rules in regards to Digital Assets	

APPENDIX E EXAMPLE OF HRC FOR DIGITAL ASSET TRANSACTIONS

Intermediaries should define thresholds for amounts according to their risk-based approach.

For clients and or counterparties that are Swiss or foreign regulated financial institutions, the thresholds shall be adapted according to the lower risk those counterparties present[1].

Client's domicile	Origin or destination of the Digital Assets	Token classification	Amount
Low-risk country	Public Wallet Addresses controlled by a Vetted VASP (other than a NPS-VASP)	Utility or investment token	CHF xxx
		Payment token	CHF xxx
	Other Public Wallet Addresses	Utility or investment token	CHF xxx
		Payment token	CHF xxx
Medium-risk country	Public Wallet Addresses controlled by a Vetted VASP (other than a NPS-VASP)	Utility or investment token	CHF xxx
		Payment token	CHF xxx
	Other Public Wallet Addresses	Utility or investment token	CHF xxx
		Payment token	CHF xxx
High-risk country	Public Wallet Addresses controlled by a Vetted VASP (other than a NPS-VASP)	Utility or investment token	CHF xxx
		Payment token	CHF xxx
	Other Public Wallet Addresses	Utility or investment token	CHF xxx
		Payment token	CHF xxx
Countries other than those referred to in another category	Public Wallet Addresses controlled by a Vetted VASP (other than a NPS-VASP)	Utility or investment token	CHF xxx
		Payment token	CHF xxx
	Other Public Wallet Addresses	Utility or investment token	CHF xxx
		Payment token	CHF xxx
Special FATF countries	Public Wallet Addresses controlled by a Vetted VASP (other than a NPS-VASP)	Utility or investment token	CHF xxx
		Payment token	CHF xxx
	Other Public Wallet Addresses	Utility or investment token	CHF xxx
		Payment token	CHF xxx

The lists of low-risk countries, medium-risk countries and high-risk countries should be determined by the Intermediary based on generally acceptable sources, such as the Basel AML Index, FATF's evaluations, the Corruption Perceptions Index, the EU Commission's list of high-risk third-country jurisdictions and sanctions imposed by United Nations (UN), Switzerland, the EU, the U.S.A and/or the U.K. In case the Intermediary is unable to identify with an appropriate level of comfort that the Public Wallet Address is held with a Vetted VASP (other than a NPS-VASP), the Intermediary should consider that the Public Wallet Address falls within the "Other Public Wallet Addresses" category. In case the classification of a Digital Asset is uncertain, such Digital Asset shall be considered as a Payment Token.

1 Regulated financial intermediaries are banks, brokers or asset managers authorized to hold client funds located in a jurisdiction with appropriate regulation and supervision from an AML/CTF perspective (as defined in the AMLO-FINMA).

CMTA Digital Assets - AML Standards for
Financial Intermediaries

Version: 2.0
Published: September 10, 2024

Capital Markets and Technology Association
Route de Chêne 30
1208 Genève

admin@cmta.ch
+41 22 73 00 00

cmta.