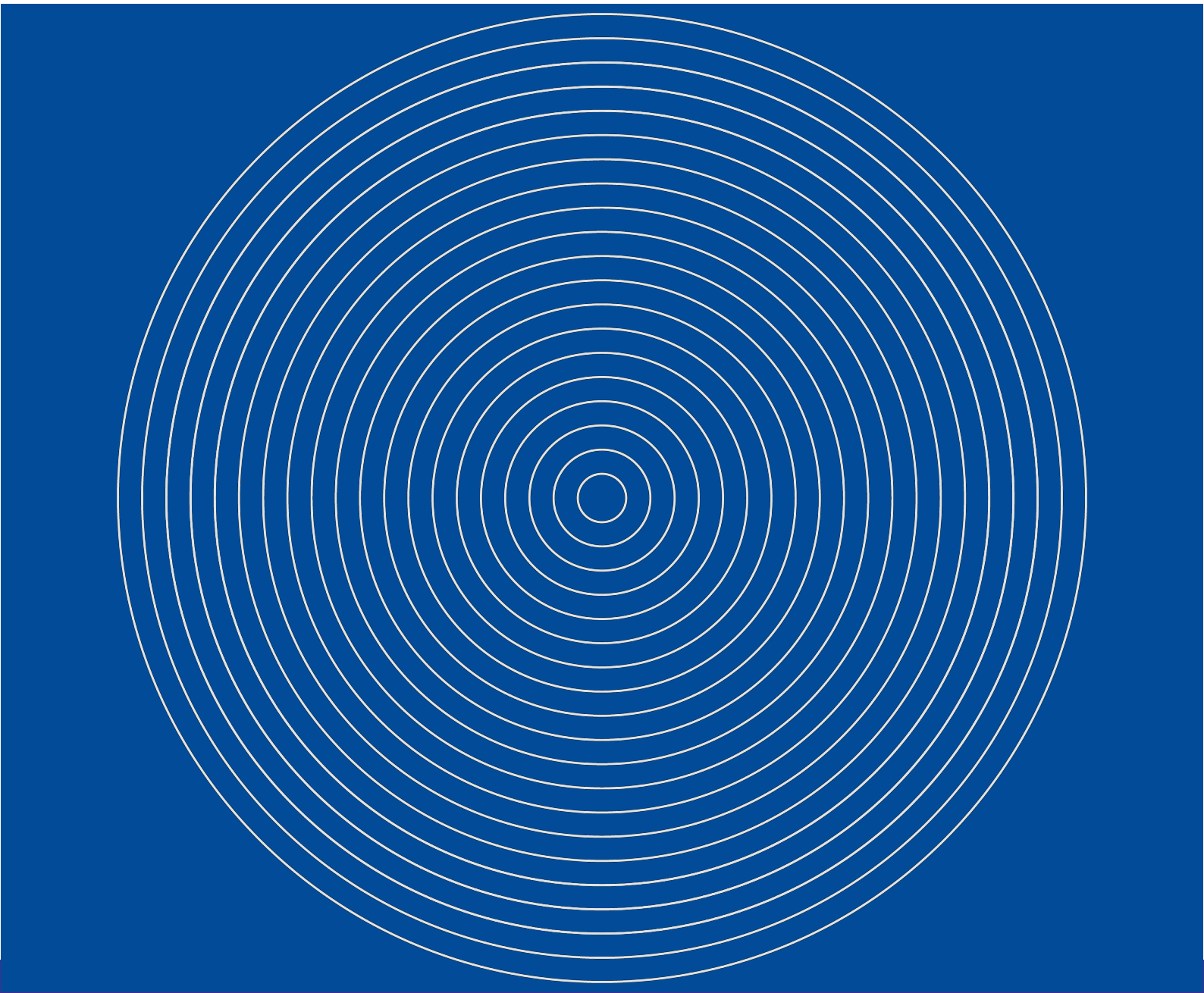
cmta.

Digital Assets
AML STANDARDS
for Issuers

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 specifically the AML policies and procedures for Issuers of Digital Assets (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 issuances of Digital Assets after the entry into force of these Standards or in situations where the due diligence on a Contributor needs 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 Issuers 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 Issuers 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 Issuers

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

These Standards describe the recommended framework that an Issuer planning to receive contributions based on, or in relation to, the issuance of Digital Assets using Distributed Ledger Technologies may elect to implement.

CHAPTER 2. GENERAL PROVISIONS

Section 1. Applicability of financial market laws and regulations

1. The Issuer shall clarify whether its business model, in particular the issuance and/or offering of Digital Assets (the "**Offering**"), triggers any regulatory approval, licensing or registration requirements, in particular:

   (a) as a Financial Intermediary; or

   (b) otherwise as a business subject to the AMLA and/or financial market supervision in accordance with Art. 3 of the Federal Act on the Swiss Financial Market Supervisory Authority (FINMASA) under any of the applicable Swiss financial market laws (as defined in FINMASA).

   FINMA circulars, published practice and guidelines shall be duly taken into account in this regard.

2. If the Issuer is a Financial Intermediary or is otherwise subject to the AMLA:

   (a) the Issuer may elect to apply the Standards in addition to its obligations under the AMLA and its implementing provisions, in particular to implement a risk-based approach; and

   (b) the AMLA and its implementing regulations shall in any event prevail over the Standards.

3. If the Issuer is not subject to the AMLA, the Issuer may elect to voluntarily apply the Standards in order to manage its reputational risks and/or satisfy the requirements of Financial Intermediaries with which the Issuer maintains or may wish to establish a business relationship.

Section 2. Effect of election to apply the Standards

1. The Issuer that has elected to apply the Standards and wishes to claim compliance with the Standards, shall apply all of the provisions of the Standards.

CHAPTER 3. LIST OF EXCLUDED JURISDICTIONS

Section 1. Preparation of the list

1. The Issuer shall establish a list of Excluded Jurisdictions that will serve as a key element of its risk-based approach and for the due diligence procedures described in the Standards. An "**Excluded Jurisdiction**" means a jurisdiction in which, for legal, regulatory or other reasons, the Offering cannot be conducted and/or the Issuer has determined that contributions from such Excluded Jurisdictions shall not be accepted.

2. The preparation of the list of Excluded Jurisdictions shall take into consideration all sanctions or other restrictions

applicable in Switzerland, as well as in each jurisdiction where the Issuer conducts or intends to conduct its business or the Offering.

Section 2. Effect

1. The Issuer shall exclude from the Offering any person or entity participating in the Offering (each a "**Contributor**") whose domicile or registered address is in an Excluded Jurisdiction.

Section 3. Updates

1. The Issuer shall ensure that, throughout the Offering, the list of Excluded Jurisdictions is maintained up-to-date.

CHAPTER 4. IDENTIFICATION OF THE CONTRIBUTOR

Section 1. General principles

1. The Issuer shall:

   (a) identify the Contributor prior to any participation of the Contributor in the Offering, and appropriately record the identity of the Contributor; and

   (b) verify and appropriately document the identity of the Contributor:

      (1) in accordance with the applicable requirements of the AMLA and its implementing regulations, if the Issuer is subject to the AMLA, it being understood that the Issuer may implement some of the risk-based approach elements set out in the Standards to the extent compatible with the AMLA; and/or

      (2) by applying a risk-based approach depending on the amount of the Contributor's contemplated contribution in the Offering (the "**Contribution Amount**"), provided that if the actual contribution were to exceed the Contribution Amount, additional verifications shall be conducted if need be.

2. The following information and documents shall be recorded as a minimum as part of the onboarding of the Contributor:

   (a) for natural persons (i.e., individuals):

      (1) first name(s) and last name(s);

      (2) date of birth;

      (3) all nationalities;

      (4) current domicile address (i.e., permanent residence address); and

      (5) document used to verify the identity.

   (b) for entities (incl. corporations, partnerships, trusts, foundations, and other legal forms or arrangements):

      (1) registered name;

(2) current registered office address, and business address (if different);

(3) document used to verify the identity; and

(4) details in accordance with § (a) above for each natural person acting on behalf of the Contributor to participate in the Offering;

(c) for all Contributors, depending on the manner in which the Contribution Amount is expected to be paid, either:

(1) a bank account number (IBAN); or

(2) a Distributed Ledger Account Number (the "**Public Wallet Address**") and such other information as may be necessary to conduct a Wallet Ownership Verification, as appropriate.

3. A Contributor whose identity has been verified by the Issuer in relation to an Offering does not need to be identified again for a subsequent Offering by the same Issuer within six (6) months from the start of the previous Offering, provided that the details relating to the subsequent contribution remain the same.

Section 2. Natural persons

1. The verification of the identity of a Contributor who is a natural person shall follow a risk-based approach depending on the Contribution Amount and shall require as a minimum the following information and/or documents from the Contributor:

(a) Tier 1 Less than CHF 15'000 (or the equivalent in any other currency)

(1) a simple copy (incl. electronic copy such as a scan or photograph) of an official identification document with a photograph;

(2) a photograph (selfie) of the Contributor, holding such Contributor's official identification document and a document with the current date (e.g., self-issued note with current date); and

(3) confirmation of the Contributor's current domicile address (e.g., by means of geolocalisation, control of the mobile phone number or localisation.

(b) Tier 2 Equal to or higher than CHF 15'000 and less than CHF 100'000 (or the equivalent in any other currency):

(1) a simple copy (incl. electronic copy such as a scan or photograph) of an official identification document with a photograph;

(2) a photograph (selfie) of the Contributor, holding such Contributor's official identification document and a document with the current date (e.g., self-issued note with current date); and

(3) confirmation of the Contributor's current domicile address by the provision of a simple copy (incl. electronic copy such as a scan or photograph) of a recent proof of residence (i.e., less than 6 months), such as:

(i) power, water, telephone invoice or another utility bill; or

(ii) tax or another official invoice;

or by such other means permitted by the CDB or FINMA Circular 2016/7 "Video and online identification".

(c) Tier 3 Equal to or higher than CHF 100'000 (or the equivalent in any other currency):

(1) a certified copy of an official identification document with a photograph (or equivalent), obtained by either of:

(i) a face-to-face meeting;

(ii) an identification via a video-conference; or

(iii) a certification by a person or entity authorized to provide authentication pursuant to the CDB;

or by such other means permitted by the CDB or FINMA Circular 2016/7 "Video and online identification".

(2) confirmation of the Contributor's current domicile address by the provision of a simple copy (incl. electronic copy such as a scan or a photograph) of a recent proof of residence (i.e., less than 6 months), such as:

(i) power, water, telephone invoice or another utility bill; or

(ii) tax or another official invoice;

or by such other means permitted by the CDB or FINMA Circular 2016/7 "Video and online identification".

2. Only official identification documents of the respective issuing jurisdictions, which are valid and include a photograph, shall be used to verify the identity of the Contributor. The presence of a machine-readable zone or optical security features (such as holographic-kinematic features or printing elements with a tilting effect) on the identification document may be set as additional requirements by the Issuer, but are not required by the Standards.

Section 3. Entities

1. For the purpose of the verification of the identity of a Contributor which is an entity, the Issuer shall obtain from the Contributor at least (depending on the legal form of the entity and the jurisdiction of incorporation):

(a) a certificate of incorporation, commercial register extract or equivalent, issued by an official registrar or public database;

(b) a copy of the articles of association or equivalent constitutive documents of the entity; and

(c) documentation establishing the identity and powers of the individuals acting on behalf of the Contributor for the purpose of participating in the Offering;

or equivalent documentation.

2. Documentation provided by the Contributor may not be more than twelve (12) months old.

3. The Issuer shall identify the natural person(s) acting on behalf of the Contributor which is an entity in accordance with the requirements set out in Chapter 4, Section 2 above.

CHAPTER 5. ESTABLISHING THE IDENTITY OF THE BENEFICIAL OWNER(S)

Section 1. General principles

1. In addition to the identification of the Contributor, the Issuer shall obtain from each Contributor a statement confirming the identity of the beneficial owner(s) of the contribution to be made by the Contributor in the Offering

and/or the controlling person(s) of the Contributor, as a minimum:

(a) Tier 1: either:

(1) if the Contributor is an entity (unless an exception applies in accordance with Section 4 below); or

(2) irrespective of the identity and type of Contributor, in situations where the Issuer has doubts that the Contributor is the beneficial owner of the assets;

(b) Tier 2 and Tier 3: in all instances, unless an exception applies in accordance with Section 4 below.

2. The beneficial owner and/or controlling person shall be a natural person (i.e., individual) and not an entity.

3. The declaration as to the beneficial owner(s) may be made in writing or in any other form demonstrable via human readable text, provided that such declaration may be attributed to the Contributor by verifiable means. The declaration may be provided as an electronic copy such as a scan or a photograph.

4. The Issuer shall identify the beneficial owner(s) and/or controlling person(s) by obtaining at least the following information and document in respect to each such person:

(a) first name(s) and last name(s);

(b) date of birth;

(c) all nationalities;

(d) current domicile address (i.e., permanent residence address); and

(e) copy of official identification document with a photograph.

5. The Issuer shall apply the relevant provisions of the CDB by analogy, to the extent appropriate.

Section 2. Natural persons

The Issuer may rely on a declaration or representation by the Contributor who is a natural person that the Contributor is the beneficial owner of the Contribution Amount including where such declaration or representation is included in the Offering documentation and not on a separate document.

Section 3. Entities

1. The Issuer shall establish and document the identity of the beneficial owner(s) and/or controlling person(s) of a Contributor that is an entity as follows:

(a) Operating company: the Issuer shall identify the controlling person(s) of an operating company in lieu of the beneficial owner(s) in the following order of priority:

(1) natural persons with voting rights or ownership of capital of 25% or more in the Contributor;

(2) failing those, natural persons who exercise control over the Contributor by other discernible means; or

(3) if no controlling persons can be determined, the highest managing director of the Contributor is to be identified as a substitute for the controlling person.

(b) Domiciliary company: the Issuer shall identify the ultimate beneficial owner(s) of a domiciliary company without

applying any threshold. For the purposes of the Standards, the term "domiciliary company" includes any entity, either Swiss or foreign, irrespective of its legal form or structure, that is not an operating company (i.e., which generally conducts no business, and no employees, and/or has no own premises).

2. For other situations or in case of doubt as to the appropriate identification measures to be implemented, in particular for Contributors that are trusts, foundations or other types of entities not otherwise covered in this Section 3, the Issuer shall apply the relevant provisions of the CDB by analogy, to the extent appropriate.

Section 4. Exceptions

1. Generally, no identification of beneficial owner(s) and/or controlling person(s) by the Issuer shall be required for:

   (a) entities that are regulated financial intermediaries such as banks, securities firms, portfolio managers, collective asset managers and insurance companies, provided that they are incorporated and regulated in a FATF member jurisdiction;

   (b) entities that are listed on a recognised stock exchange operating from a FATF member jurisdiction;

   (c) governmental authorities and entities; or

   (d) any other instances where an exemption is applicable under applicable AML laws.

2. The Issuer shall appropriately document any such exceptions.

CHAPTER 6. DUE DILIGENCE PROCEDURES AT THE TIME OF ONBOARDING

Section 1. Screening against databases

1. The Issuer shall screen the first and last name(s), respectively registered name, of each of:

   (a) the Contributor;

   (b) the natural person(s) acting on behalf of the Contributor (if an entity); and/or

   (c) the beneficial owner(s) and/or the controlling person(s)

   against appropriate databases covering at least relevant information on sanctions, politically exposed persons and adverse media.

2. The Issuer shall review the results of the screening to determine whether to reject a particular Contributor, following a risk-based approach. In principle the Issuer shall exclude any Contributor from the Offering in case of:

   (a) a confirmed positive hit on any of the databases (e.g., sanctions) on the Contributor, any beneficial owner, controlling person or natural person(s) acting on behalf of the Contributor; or

   (b) reasonable doubts which the Issuer was not in a position to adequately address or clarify.

3. The Issuer shall appropriately document the screening, the results thereof and any clarifications conducted, respectively the assessment and decision as to the admission or exclusion of a Contributor from the Offering.

Section 2. Consistency checks

1. The Issuer shall conduct consistency checks on a risk-based or sample basis, including as a minimum as follows:

   (a) consistency of the elements of the official identification document;

   (b) consistency of the photograph on the official identification document and the selfie; and

   (c) general consistency of other information provided (e.g., domicile address and address on utility bill).

2. In case of any doubts or suspicions, the Issuer shall perform additional clarifications, including by means of additional documents or information to be requested from the Contributor, respectively by checking documents or information provided against databases.

3. The Issuer shall appropriately document the consistency checks and the results thereof.

4. The Issuer shall exclude any Contributor from the Offering in case of inconsistency which the Issuer was not in a position to adequately clarify.

Section 3. Multiple participations

1. The Issuer shall put in place controls to identify cases where the same Contributor participates several times in the Offering. This shall be done by checking whether the same identification information or document are used for several contributions, by way of technical means (i.e. same Public Wallet Address, the same IP address or any other technical solutions).

2. Controls may also include the review of the selfie.

3. The Issuer shall:

   (a) prevent a Contributor from participating multiple times in the same Offering; or

   (b) ensure that the relevant due diligence requirements take into consideration the aggregate Contribution Amount and obtain appropriate explanations on the Contributor's reasons for participating multiple times.

Section 4. Clarifying the origin of funds

1. The Issuer shall obtain from the Contributor a confirmation whether the Contribution Amount will be in "**Fiat Currencies**" or in Digital Assets.

2. With respect to contributions in Fiat Currencies, the Issuer shall obtain the details of the bank account number (IBAN) of the Contributor and determine whether such bank account is acceptable, in particular in view of the list of Excluded Jurisdictions. Such information shall be duly recorded in the Issuer's systems in order to enable the reconciliation procedures referred to in Chapter 7, Section 1 to be performed.

3. With respect to a contribution by means of Digital Assets, the Issuer shall:

   (a) obtain the Public Wallet Address that the Contributor intends to use for the contribution, if applicable and known to the Contributor;

   (b) in all instances, perform a "**Blockchain Forensic Analysis**" of the stated Public Wallet Address and/or of the Public Wallet Address from which the actual contribution is received via the systems of an acceptable

Blockchain Forensic Analysis provider. The information and results of the Blockchain Forensic Analysis shall be duly recorded in the Issuer's systems in order to enable the reconciliation procedures referred to in Chapter 7, Section 1 to be performed; and

(c) in all instances, carry out a Wallet Ownership Verification.

Section 5. Additional information

1. The Issuer shall obtain, review and appropriately record the following additional information on the Contributors with Tier 3 Contribution level:

   (a) employment status (position, company, business industry, etc.);

   (b) source of funds to be contributed and source of wealth of the Contributor; and

   (c) information on any important public function.

2. Obtaining this additional information is recommended, but not mandatory, for Contributors with Tier 2 Contribution level.

CHAPTER 7. DUE DILIGENCE PROCEDURES AT THE TIME OF CONTRIBUTION

Section 1. Reconciliation with respect to the Contribution Amount

1. The Issuer shall maintain a system enabling the identification of cases where the Contributor transferred funds in an amount higher than the Contribution Amount.

2. When identifying such inconsistencies, the Issuer shall either:

   (a) subject the Contributor to the requirements applicable to the contribution tier level corresponding to the actual Contribution Amount; or

   (b) return the funds in excess of the upper limit of the contribution tier level for which the due diligence procedures performed on the Contributor were completed to the Issuer's satisfaction.

3. The Issuer shall document the process and outcomes of the reconciliation procedures.

Section 2. Reconciliation with respect to the origin of the funds

1. The Issuer shall ensure that invested funds (be they Fiat Currencies or Digital Assets) only come from the bank account, respectively the Public Wallet Address indicated as part of the onboarding.

2. In case of discrepancy, the Issuer shall either:

   (a) reject the invested funds (or, send them back, in the case of Digital Assets); or

   (b) carry out the appropriate due diligence procedures with respect to these new elements and obtain from the Contributor adequate explanations.

3. The Issuer shall document the process and outcomes of the reconciliation procedures.

CHAPTER 8. DUE DILIGENCE PROCEDURES AT THE EXERCISE OF A RIGHT OR A CLAIM REPRESENTED BY A LEDGER-BASED SECURITY

Section 1. Scope

This section applies to Issuers of ledger-based securities in accordance with art. 973d to 973i of the Swiss Code of Obligations ("**CO**"), when a holder of such ledger-based securities requests the performance of a right or a claim represented by the ledger-based security.

Section 2. Issuers subject to the AMLA

1. For Issuers of ledger-based securities that are subject to the AMLA:

   (a) If the current holder of the ledger-based security is the Contributor, the Issuer should apply a risk-based approach to determine which additional clarifications (if any) are required before rendering performance on the right or claim. For the purposes of such risk-based approach, the Issuer may take into account:

      (1) whether the ledger-based security has been transferred out of the Public Wallet Address used by the Contributor for the contribution, or has remained in such Public Wallet Address;

      (2) the jurisdiction in which the Contributor resides or is headquartered;

      (3) the general level of risk presented by the Contributor.

   (b) If the current holder of the ledger-based security is different from the Contributor, then Chapters 4, 5 and 6 above apply by analogy to the identification of the current holder of the ledger-based security.

2. On the basis of the results of the identification or clarifications, the Issuer may:

   (a) refuse to render performance until so ordered by a competent court or authority;

   (b) report the case to the MROS in accordance with the AMLA if the Issuer knows or has reasonable grounds to suspect that the holder of the ledger-based security is connected to criminal offences or terrorist organizations.

Section 3. Issuers not subject to the AMLA

1. For Issuers of ledger-based securities that are not subject to the AMLA (such as issuers of tokenized shares) who have elected to apply the Standards, the Issuer should apply a risk-based approach in relation to the identification of the holder of a ledger-based security before rendering performance on the right or claim. For the purposes of such risk-based approach, the Issuer may apply an approach similar to the one described in Section 2 above.

2. On the basis of the identification procedures and any additional information collected or obtained (if any), the Issuer may:

   (a) refuse to render performance until so ordered by a competent court or authority;

   (b) alert the competent authorities if the Issuer knows or has reasonable grounds to suspect that the holder of the ledger-based security is connected to criminal offences or terrorist organizations.

Section 4. Sanctions

1. Although sanctions compliance is outside the scope of the Standards, the Issuer should refuse performance in accordance with any applicable sanctions regime.

CHAPTER 9. VARIOUS

Section 1. Records

The Issuer shall keep appropriate records of all information and documents obtained during the procedures set forth in the Standards and in all cases, in compliance with the applicable law.

Section 2. Delegation to third parties

1. The Issuer may delegate the performance of all or part of the due diligence procedures set out in the Standards to a service provider, provided that:

   (a) the delegation is formalised in writing or in any other form demonstrable via human readable text; and

   (b) the service provider has the requisite professional knowledge and technology to perform the due diligence procedures.

2. The Issuer shall have the right to obtain from the service provider all information or documents collected as part of the performance of the due diligence procedures.

Section 3. Renewal of due diligence procedures

1. The Issuer should renew, in full or in part, the due diligence procedures in relation to the then current holder of Digital Assets at least prior to:

   (a) any new Offering to which the Contributor participates, if:

      (1) the preceding Offering by the same Issuer dates back more than six (6) months; or

      (2) the details of the Contributor change in any respect, in particular if the source Public Wallet Address or IBAN for the contribution are different;

   (b) any payment or distribution in Fiat Currency and/or Digital Assets to holders of any Digital Assets previously issued by the Issuer, such as corporate actions, dividends, interest or redemption payments.

2. The renewal of due diligence procedures shall be made by applying the requirements applicable at the time of the renewal, as may have been amended or updated since the original contribution. In particular, the identification or renewal of the identification of the holder of Digital Assets shall be performed in accordance with Chapter 8.

3. This Section does not apply to verifications relating to the origin of funds, which must be checked at the time of each contribution.

Section 4. Sanctions Screening

1. Although sanctions compliance is outside the scope of the Standards, unless new relevant sanctions are adopted or other restrictions introduced:

   (a) due diligence procedures performed in relation to a Contributor on the basis of a previously adopted list of Excluded Jurisdictions are not required to be renewed solely because of an update of the list of Excluded Jurisdictions; and

   (b) the Issuer should adopt a risk-based approach to ongoing screening of Contributors' Public Wallet Addresses against known sanctioned Public Wallet Addresses (e.g., OFAC database), to be implemented by adopting an automated Public Wallet Addresses screening via tools for Blockchain Forensic Analysis.

CHAPTER 10. EXAMPLE OF RISK-BASED APPROACH IMPLEMENTATION

A synthetic example of a possible risk-based approach implementation that an Issuer which is not subject to AMLA may decide to adopt is enclosed as **Appendix B**.

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 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 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; • such Public Wallet Addresses are known to be associated with money laundering, financing of terrorism or cybercrime (e.g., stolen Digital Assets); and/or • such Public Wallet Addresses are known to be associated with transactions relating to sanctioned countries or persons. 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.
Contribution Amount	Amount of the Contributor's contemplated contribution in an Offering.
Contributor	Any person or entity participating in an Offering.
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.

Defined term	Definition
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 (incl. Cryptocurrencies), Utility Tokens and Asset Tokens.
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 jurisdictions shall not be accepted, respectively performace of rights or claims in favour of holders of Digital Assets of such excluded jurisdictions shall be rejected.
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.
Issuer	Person or entity issuing and offering Digital Assets.
MROS	Money Laundering Reporting Office Switzerland (https://www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/geldwaescherei.html).
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 cryptocurrency 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 Issuers.

Defined term	Definition
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 Tokens	See Token.
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 Issuer from the person's own Public Wallet Address to a specific Public Wallet Address designated by the Issuer within a specified time period (so-called "satoshi test"); • the relevant person gives to the Issuer prior notice of the transaction and the desired amount to be transferred to the Issuer, whereupon the Issuer will notify a Public Wallet Address 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 Issuer or the Issuer's agent (e.g., service provider).

APPENDIX B - EXAMPLE OF RISK-BASED APPROACH IMPLEMENTATION

Applicable for Contributors who are natural persons (i.e., individuals).

The table in Appendix B is of exemplary nature and does not constitute minimum requirements as the information/ documents required and respective checks may vary applying a risk-based approach adopted by the Issuer in accordance with the Standards .

Tier level	Information/document required	Checks
Tier 1 (less than CHF 15'000)	First name(s), last name(s) and date of birth	Against sanctions, politically exposed persons and adverse media databases
	Copy of an identification document	Coherence of the elements of the identification document and consistency with selfie
	Domicile address (including country)	Against list of Excluded Jurisdictions
	Contribution Amount	Tier definition
	Email address	Usability
	Phone number	Consistency of address
	Origin of the funds: Public Wallet Addresses (from which Digital Assets will be transferred) or Bank account (IBAN) owned by the Contributor in an accepted country (account from which Fiat Currencies will be transferred)	Blockchain Forensic Analysis Acceptability
	Selfie (of the Contributor holding his/her ID and a post-it with the current date)	Consistency with the photograph on the identification document
	IP address	Consistency of the domicile address via geo-localisation
	Combination of information/ documents and matching elements collected as per above list	Identify multiple participations by the same Contributor
Tier 2 (less than CHF 100'000)	All Tier 1 information and documents (other than IP address)	See Tier 1 above (except checks on the phone number and IP address)
	Employment status (position, sector, company)	Background of the Contributor
	Important public function (if yes, details)	Background of the Contributor
	Source of funds	Background of the Contributor
	Utility bill (not older than 6 months)	Consistency of the domicile address
	Declaration as to beneficial owner(s)	Review if properly filled in
Tier 3 (CHF 100'000 or more)	All Tier 1 and Tier 2 information and documents (other than selfie and IP address)	See Tier 1 and Tier 2 above (except checks on the phone number, selfie and IP address)
	Video-conference	Identity and background of the Contributor via a KYC interview

cmta.

Digital Assets -
AML STANDARDS for **Issuers.**

CMTA Digital Assets - AML Standards for Issuers

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.