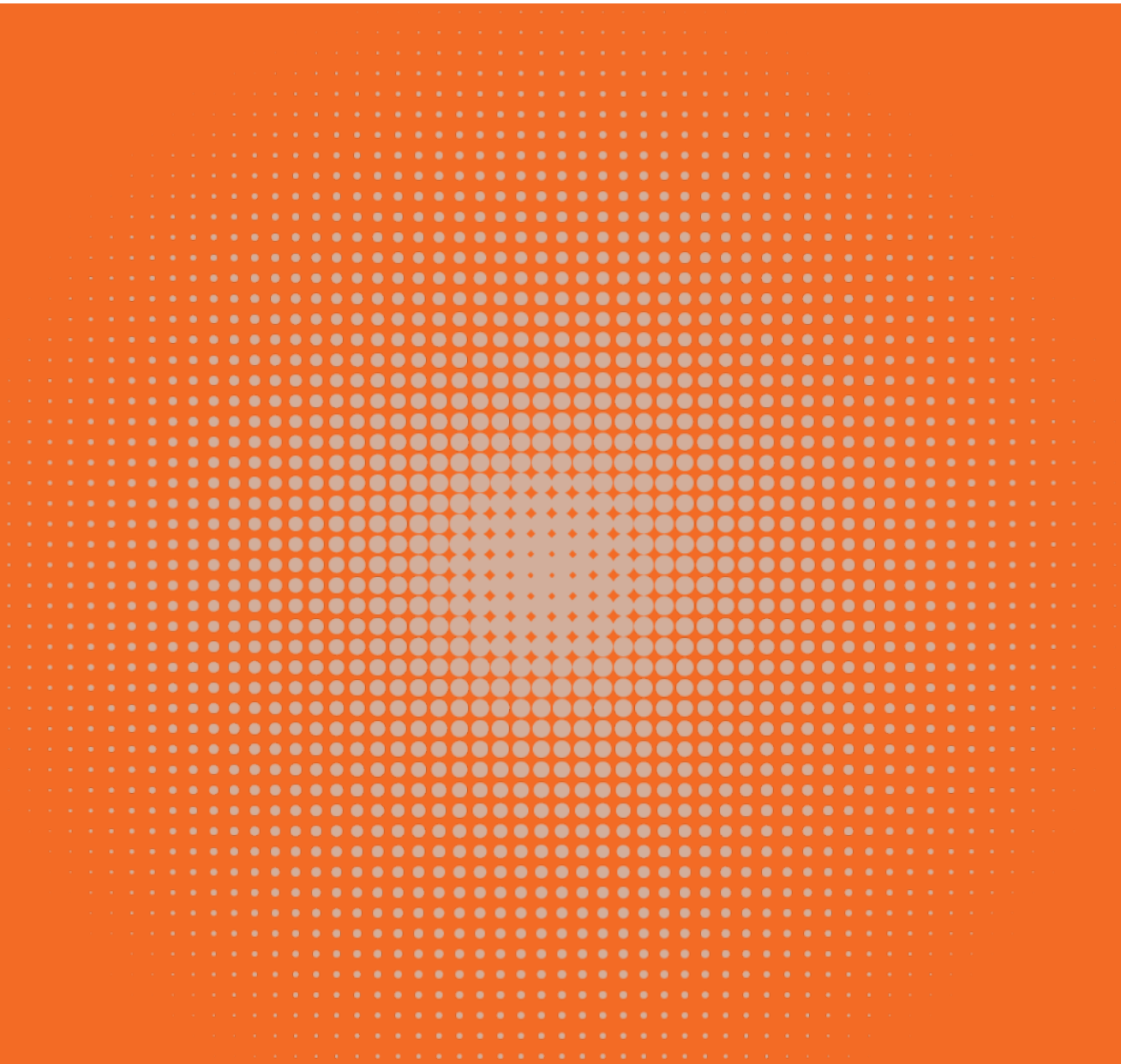
cmta.

STANDARD

for the tokenization of debt instruments using distributed ledger technology.

May 2025



Standard for the tokenization of debt instruments using distributed ledger technology.

Capital Markets and Technology Association
Route de Chêne 30
1208 Genève

Approved: May 19, 2025

admin@cmta.ch
+41 22 73 00 00

Table of Contents

1. INTRODUCTION 4

§ 1.1 Background 4
§ 1.2 Scope 4
§ 1.3 Terminology 5
§ 1.4 Compliance with this standard - Certification 6

2. TOKENIZATION OF DEBT INSTRUMENTS – REQUIREMENTS AND RECOMMENDATIONS 7

§ 2.1 Valid existence of the issuer 7
§ 2.2 Eligibility of the instruments 7
§ 2.3 Tokenization process governed by Swiss law 7
§ 2.4 Tokenization carried out in compliance with Swiss law 8
§ 2.5 Publication of information on the terms and conditions of the tokenized Instruments, distributed ledger and smart contract 10
§ 2.6 Valid issuance 13
§ 2.7 Deployment of the smart contract on the distributed ledger and allocation of the tokens to Instrument holders 13

3. POST-TOKENIZATION ACTIONS 13

§ 3.1 Identification of holders - Whitelisting features 13
§ 3.2 Tokenized Instruments as intermediated securities 15
§ 3.3 Switch to non-tokenized Instruments or to new tokens 16
§ 3.4 Corporate actions 16
§ 3.5 Cancellation of tokens when the relevant private key has been lost or stolen 16

Table of Appendices

Appendix 1: CMTA template tokenization terms and information document 18
Appendix 2: Main features of a smart contract for the tokenization of Instruments 22
Appendix 3: Additional terms for *ex post* controls – Register of Holders 25
Appendix 4: Resolutions for the tokenization of Securities 29

1. INTRODUCTION

§ 1.1 Background

In 2021, the Capital Markets and Technology Association ("**CMTA**") published its "Standard for the tokenization of shares of Swiss corporations using the distributed ledger technology", a step-by-step guide to issuing equity securities of companies organized under the laws of Switzerland ("**Swiss Issuers**") in the form of "ledger-based securities", as this term is defined by Swiss law (the "**Equity Standard**"). The Equity Standard describes the manner in which equity securities of Swiss Issuers can be associated with digital tokens registered in a distributed ledger having certain characteristics defined by the relevant provisions of Swiss law (namely: Articles 973*d et seq.* of the Swiss Code of Obligations ("**CO**")), so that the relevant securities cannot be transferred without the relevant token and *vice versa*.

Under the Equity Standard, the issuance of equity rights in the form of ledger-based securities required the use of a smart contract, capable of generating digital tokens with certain properties that could be registered on a distributed ledger.

In January 2022, CMTA published the CMTA Token ("**CMTAT**"), a smart contract framework designed specifically for the creation of ledger-based securities. The CMTAT consists of open-source computer code and explanatory materials published by CMTA under Mozilla Public License 2.0. It has been conceived as a framework, which can be implemented on various public blockchains (currently Ethereum and Tezos) to generate tokens that satisfy both the requirements of Swiss law for the creation of ledger-based securities and CMTA's requirements (in particular CMTA's Equity Standard's recommendations and requirements). Whilst the CMTAT can be used for the issuance of shares and other equity securities in the form of ledger-based securities, it can also be used for the creation of other forms of securities in ledger-based format.

This standard (the "**Debt Standard**") describes the manner in which certain instruments that are not equity securities can be issued in the form of ledger-based securities in compliance with Swiss law.

§ 1.2 Scope

1.2.1 Debt instruments

This Debt Standard applies to the tokenization of all forms of securities that incorporate rights or claims that are contractual in nature, as opposed to rights or claims that derive from the articles of association or other constitutive documents of the issuer and involve equity rights. It can consequently be applied for the issuance of debt instruments *stricto sensu* (such as bonds within the meaning of Article 3 lit. 3 No. 7 of the Swiss Federal Act on Financial Services of 2018, as amended (the "**FinSA**")), but also for the issuance of other forms of financial instruments within the meaning of Article 3 lit. a FinSA, such as structured products (including exchange traded products), and other derivative instruments[1].

1.2.2 Standardization and fungibility

This Debt Standard applies primarily to debt instruments that characterize as "securities" as defined by Swiss law,

1 Units in collective investment schemes may characterize as equity or debt instruments for what regards their tokenization. Their issuance or distribution may also be subject to specific regulatory requirements, which are not discussed in the Equity Standard or this Debt Standard.

i.e., that are "standardized" and are "suitable for mass trading"[2]. However, this Debt Standard can also be used for the tokenization of financial instruments that do not qualify as securities.

1.2.3 Transferability

This Debt Standard applies to transferable instruments, i.e., an instrument that can be associated with a digital token recorded on a distributed ledger, in such a way that the Instrument cannot be transferred without the token and vice versa. This requires that the instrument be generally transferable, and that the legal title to the instrument can be passed through the transfer of a digital token on a distributed ledger. This means that instruments whose transfer is subject to a particular form, registration in a central registry (e.g., a land registry) or approval by a third party, cannot be tokenized under this Debt Standard.

The existence of contractual transfer restrictions in the terms and conditions of a particular debt instrument does not, however, make such instruments ineligible for tokenization under this Debt Standard. For example, the fact that the transfer of a particular instrument requires – according to its terms – the consent of the issuer or the transfer in a certain minimum denomination (e.g., CHF 5,000), does not result in the instrument becoming incapable of being issued as a ledger-based security[3].

If the contractual terms and conditions of a particular financial instrument include transfer restrictions, the issuer must however make sure that the smart contract governing the relevant tokens adequately reflects those restrictions, so that the tokens can technically only be transferred on the ledger if the contractual transfer restrictions have been complied with (see § 3.1 below).

1.2.4 Swiss and foreign issuers – Applicable law and jurisdiction of Swiss courts

This Debt Standard can be used by both Swiss Issuers and issuers that are organized under laws other than Swiss law. The issuer must however have the capacity under the laws by which it is governed to issue transferable financial instruments capable of being tokenized under this Debt Standard (see Section 1.2.3 above). If the issuer is not a Swiss Issuer or if the relevant instrument is governed by a law other than Swiss law, the tokenization terms must declare Swiss law as governing for the tokenization process and form of securities (namely: ledger-based securities pursuant to Articles 973*d et seq.* CO), and grant jurisdiction to Swiss courts for matters related to the tokenization process (see § 2.3 below).

§ 1.3 Terminology

In this Debt Standard, the term:

(i) "**Instrument**" refers to the non-equity financial instrument that is the subject matter of the tokenization process;

(ii) "**issuer**" refers to both Swiss Issuers and issuers organized under laws other than Swiss law; and

(iii) "**ledger-based instruments**" or "**ledger-based securities**" refers to Instruments issued in ledger-based form within the meaning of Article 973*d et seq.* CO.

---

2 Article 3 lit. b FinSA.

3 From a legal perspective, this results from the fact that the transfer restriction derives in such a case from the contractual terms and conditions of the relevant instrument, and not from the structure of the ledger on which the tokens associated with the instruments are recorded. The transfer restriction does consequently not – per se – infringe the requirements that Article 973*d* para. 2 No. 1 CO imposes on any ledger supporting ledger-based securities.

§ 1.4 Compliance with this standard - Certification

1.4.1 Requirements and recommendations

This document outlines the requirements for the tokenization of Instruments under Swiss law as well as CMTA's recommendations in this respect. Issuers who wish to follow this standard must satisfy the requirements and follow the recommendations set forth herein.

1.4.2 Certification

Issuers that have tokenized Instruments pursuant to this Debt Standard can obtain a certification from CMTA. The process to obtain a certification is briefly described below, but is described in further detail in the regulations of CMTA's certification mark relating to this standard, which can be consulted at www.cmta.ch/certification/cmta-tokenized-debt.

The certification is available in two formats: a stand-alone certification and a certification for a series of issuances (i.e., a program). The stand-alone certification means that a specific Instrument obtains certification from CMTA. The certification for programs allows issuers to obtain a CMTA certification for multiple Instruments. To do so, an issuer is required to submit a "tokenization manual", i.e., a collection of internal procedures of the issuer that will be relied upon to tokenize Instruments in compliance with this Debt Standard. If the procedures are consistent with this Debt Standard, the issuer obtains a certification that is valid for all Instruments issued in compliance with those procedures (without CMTA issuing a dedicated confirmation for each instrument).

The certification entitles the issuer to use CMTA's certification mark "CMTA Tokenized Debt" (for a stand-alone certification) or "CMTA Tokenized Debt (Program)" (for a program certification). A certification is valid for a certain time, which may be shorter than the Instrument's lifespan, though it can be renewed. A certification must be renewed in the event of any material change, including but not limited to the smart contract, amendments to the transferability conditions, or any developments in the applicable legal or regulatory framework that may affect compliance with the Debt Standard.

To obtain such a certification, issuers must:

(i) satisfy the requirements and follow the recommendations outlined in this Debt Standard, including by using the most recent version of the CMTAT smart contract (as available at https://github.com/CMTA/CMTAT) or another smart contract recognized by CMTA;

(ii) retain a technology service provider recognized by CMTA (the list of which can be found at: www.cmta.ch/recognized-experts) to either (a) deploy the smart contract for their ledger-based securities on the relevant distributed ledger and allocate the tokens to the owners of such ledger-based securities (for a stand-alone certification), or (b) verify the issuers' procedures from a technology standpoint (for a program certification);

(iii) obtain an opinion from a legal expert recognized by CMTA (the list of which can be found at: www.cmta.ch/recognized-experts) confirming compliance with this Debt Standard; and

(iv) pay the fees for the certification process and the use of CMTA's certification mark.

CMTA certification does not constitute or substitute regulatory approval that an Instrument may require or certify compliance of the Instrument with applicable laws and regulations. Issuers remain solely responsible for ensuring that their tokenized Instruments and related processes adhere to all legal and regulatory requirements.

2. TOKENIZATION OF DEBT INSTRUMENTS – REQUIREMENTS AND RECOMMENDATIONS

§ 2.1 Valid existence of the issuer

Any financial instrument (tokenized or not) can only be validly issued by a person or entity that validly exists under the laws that govern its existence, and that is capable of issuing such financial instruments under those laws and its constitutive documents.

Requirements

01: The issuer must be duly organized and validly existing under the laws under which it is organized.

02: The issuer must have the capacity to issue the Instruments.

§ 2.2 Eligibility of the instruments

To be tokenized under this Debt Standard, an Instrument must have the properties described in § 1.2 above. In particular, it must be possible to associate the Instruments with a digital token, meaning that the laws that apply to the issuer and the laws that govern the Instrument must not prohibit the identification of the token holder by means of a digital token e.g., mandate that the Instrument be issued in the form of paper certificates.

Requirement

03: The laws that apply to the issuer and the laws that govern the Instruments (if different) must allow the Instrument to be associated with a digital token recorded on a distributed ledger.

§ 2.3 Tokenization process governed by Swiss law

This Debt Standard applies to Instruments tokenized in accordance with Swiss law. This includes Instruments issued by Swiss Issuers or non-Swiss entities, but that are governed by laws other than Swiss law. For this Debt Standard to apply in such cases, it is necessary that the issuer has chosen Swiss law for the tokenization process, i.e., for what regards the form and the transfer of the securities (but not necessarily for the other terms and conditions of the Instrument), and that the tokenization terms grant jurisdiction to Swiss courts for matters related to the tokenization process. These matters include the process through which the Instruments are associated with the tokens, and include consequently the matters relating to the proof of ownership of the relevant Instruments, and by implication the validity and effectiveness of their transfer, as well as the validity of the creation or cancellation of tokens.

Professor Florence Guillaume from the University of Neuchâtel has confirmed to CMTA that a foreign issuer can validly elect Swiss law and agree to the jurisdiction of Swiss courts for the tokenization of Instruments it issues, provided that the Instruments are capable of being tokenized under Swiss law, and that the choice of law and of the jurisdiction to Swiss courts are permissible under the laws governing the relevant issuer and its constitutive documents[4].

4 Professor Florence Guillaume's opinion is on file with the CMTA.

Requirement

04: The issuer has chosen Swiss law for the tokenization process, and the terms and conditions of the Instruments grant jurisdiction to Swiss courts for matters related to the tokenization process, including the form and transfer (acquisition, encumbrance or disposal) of the Instruments (in particular the validity of transactions conducted on the distributed ledger), as well as the validity of the creation or cancellation of tokens.

Recommendation

05: The terms and conditions governing the tokenization of the Instruments include the governing law and jurisdiction provision set forth in Appendix 1.

§ 2.4 Tokenization carried out in compliance with Swiss law

The requirements and recommendations for the tokenization of Instruments under the Debt Standard are comparable to those outlined in §§ 3.3 and 3.4 of the Equity Standard, with adjustments required to take into account the difference in nature between equity securities and debt instruments.

2.4.1 Choice of distributed ledger

Article 973*d* para 2 CO imposes certain requirements as to the distributed ledger that can be used to tokenize Instruments. From the perspective of the issuer, the requirements of Article 973*d* para 2 CO are as follows:

(i) The distributed ledger must give the holders of Instruments (but not the Issuer) the power to dispose of the Instruments through technical means.

(ii) The integrity of the distributed ledger must be protected from unauthorized modification through organizational and technical means, which may include consensus mechanisms and decentralization.

(iii) The distributed ledger itself or documentation linked to it must include a description of the terms and conditions of the tokenized Instruments, information about how the register functions and the tokenization terms.

(iv) Instrument holders must be able to consult the relevant information and ledger entries and to verify the integrity of the ledger entries relating to themselves without the assistance of third parties.

Requirement

06: The distributed ledger on which the tokenized Instruments are recorded complies with the requirements of Article 973*d* para 2 CO.

Recommendation

07: The issuer selects a distributed ledger for which CMTA provides a smart contract for tokenized Instruments. At the time of publication of this Debt Standard, these include Ethereum, Tezos and other distributed ledgers that support the Solidity programming language.

2.4.2 Minimum features of the smart contract

The smart contract governing the functioning of the tokenized Instruments must comply with two sets of requirements. On the one hand, it must meet the requirements of Article 973*d* CO. On the other hand, the features of the smart contract must generate tokens with properties that correspond to those of the tokenized Instruments. Tokens should in other words behave like Instruments and not prevent corporate actions that may have to be carried out with respect to such Instruments, such as transfer restrictions, issuance of additional Instruments (when permitted under the Instrument's terms and conditions), interest payments, redemptions, etc.

To satisfy the requirements of Article 973*d* CO, the distributed ledger selected by the issuer must meet the following conditions:

- The distributed ledger must not be controlled, directly or indirectly, by the issuer. The issuer must, in particular, not act as central validation authority for the entries made in the ledger (although the issuer can participate in a validation process – see § 3.1 below).
- The distributed ledger's functioning must include appropriate mechanisms that ensure (a) that previously validated entries are immutable, and (b) that new entries into the ledger are processed in a manner that limits the risk of unauthorized use.
- The holders of the tokens must be able to access the records of the distributed ledger and to validate the integrity of the entries in the distributed ledger that relate to them without having to request approval to do so.

The minimum functions a smart contract should have to adequately represent Instruments and comply with this Debt Standard are set forth in Appendix 2. It is possible (but not a requirement) to add features to the smart contract that support corporate actions of the issuer such as interest payments or other distributions. To comply with this Debt Standard, issuers must use a smart contract approved by CMTA. To do so, issuers may either:

(i) use the "CMTAT" smart contract provided by CMTA for the tokenization of securities; or

(ii) create a smart contract with different functions but that has been reviewed and approved by CMTA. CMTA will in such a case require that the functions of the smart contract be duly documented (e.g., published on a public repository such as Github), that the code of the smart contract be submitted to an independent security audit and that the code be made available for public inspection.

Requirement

08: The smart contract complies with the requirements of Article 973*d* para. 2 and 3 CO.

Recommendation

09: The issuer uses (i) the smart contract CMTAT in the latest version released (available at https://github.com/CMTA) or (ii) an alternative smart contract approved by CMTA.
Note: In order to be approved by the CMTA:
a: the code of the alternative smart contract must have been (i) duly

documented and (ii) submitted to a security audit carried out by a qualified expert;
b: the smart contract code must have been made available for public inspection, e.g., via blockchain explorer services or on a software development service; and
c: the audit report must be made available to the CMTA.

2.4.3 Tokenization terms

Swiss law (Article 973*d* para. 1 No. 3 and Article 973*f* para. 1 CO) requires that the transfer of tokenized instruments be governed by terms agreed between the issuer and the first token holder ("*Registrierungsvereinbarung*", "*convention d'inscription*" or "tokenization terms"), and by which any subsequent acquirer of the tokenized instruments will be bound.

The tokenization terms are the terms that determine the manner in which the tokenized Instruments (i) are associated with the digital tokens generated by means of the smart contract and (ii) can be transferred or encumbered through the transfer of the relevant tokens. They must not be confused with the terms and conditions of the Instruments themselves, which define the rights of the holder(s) of the relevant Instruments toward the issuer.

Requirement

10: The issuer must adopt tokenization terms pursuant to which the Instruments are represented by digital tokens and that specify the manner in which the tokenized Instruments can be transferred and encumbered.

Recommendation

11: The tokenization terms are adopted substantially in the form set forth in Appendix 1.

§ 2.5 Publication of information on the terms and conditions of the tokenized Instruments, distributed ledger and smart contract

Swiss law (Articles 973*d* para. 2 No. 3 and 973*i* para. 1 CO) requires that issuers of tokenized Instruments publish certain information regarding "the terms and conditions of the tokenized instruments, the functioning of the distributed ledger and the tokenization terms" ("*Der Inhalt der Rechte, die Funktionsweise des Registers und die Registrierungsvereinbarung*" / "*le contenu des droits, le mode de fonctionnement du registre et la convention d'inscription*"). The required information extends to the terms and conditions of the tokenized Instruments, the characteristics of the distributed ledger and the features of the smart contract.

2.5.1 Publication of the terms and conditions of the Instruments

The Instrument holders must be able to identify with certainty the terms and conditions of the Instrument associated with the tokens. The terms include not only the financial terms (e.g., principal amount, denomination, interest amount, and calculation, due dates), but also terms such as governing law and the courts having jurisdiction over disputes between holders of Instruments and the issuer. The tokenization terms (see Section 2.4.3 above) are part of the Instruments' terms and conditions, and must be published in the same manner as the financial terms of the Instruments.

The publication of the terms and conditions of the Instruments can be carried out in various ways. Assuming that the relevant distributed ledger's smart contract size limit permits it, the terms and conditions could be reproduced in full in

the smart contract (in plain text). It is also possible to add an identifier in the smart contract, which can take the form of:

- a "hash" (i.e., an alphanumeric string recorded on the distributed ledger) of the terms and conditions that is included in the smart contract; or
- the unique identifier / envelope number of the electronically signed version of the terms and conditions.

Where terms and conditions are not reproduced in full in the smart contract, the terms and conditions would have to also be published outside of the relevant distributed ledger (e.g., on a webpage or in a third-party repository, including one maintained by a prospectus review office). If an issuer relies on an identifier, the published terms and conditions should allow the reader to verify the identifier. For example, if an issuer adds the unique identifier of the electronically signed version of a document in the smart contract, the Issuer should publish the electronically signed terms and conditions, such that one reviewing them could ascertain that the identifier is the same as the one appearing in the smart contract.

Issuers have the possibility to include in the smart contract or refer to terms and conditions drafted in the form of "natural language" (taking the form of sentences understandable by humans) or in a "machine readable" format, including data designed for interpretation and processing by computer systems. In the latter case, it must be possible to translate the "machine readable" format into terms expressed in natural language, without such translation being subject to undue uncertainty or ambiguity.

The choice to either include the complete terms and conditions of the Instruments in the smart contract, or merely a hash or electronic signature envelope / certificate of these terms and conditions, may hinge on technical factors, such as the need to minimize the smart contract's size and thereby reduce the "gas" required for token transactions on the distributed ledger. However, for the efficient trading of tokenized Instruments, it is recommended that a core set of information (mentioned in Appendix 2) be embedded directly within the smart contract. This allows the information to be retrieved directly from the distributed ledger, eliminating the need to access external data sources.

Requirement

12: The issuer makes available to each token holder (i) the terms and conditions of the tokenized Instruments and (ii) the tokenization terms.

Recommendations

13: The terms and conditions of the Instruments (including the tokenization terms) are reproduced in full in the smart contract. Alternatively, the smart contract includes a unique identifier (whether in the form of a "hash" or of a unique identifier / envelope number of the electronically signed version of the terms).

14: If the full terms of the Instruments are not reproduced in the smart contract, the data set forth in Appendix 2 should at a minimum be recorded in the smart contract.

15: If the terms of the Instruments are expressed in a machine-readable format, the issuer must procure that those terms can be translated into terms expressed in a natural language, without such translation being subject to undue uncertainty or ambiguity.

2.5.2 Information on the functioning of the distributed ledger and smart contract

Article 973*d* para. 2 No. 3 and Article 973*i* para. 1 No. 2 CO do not require that the functioning of the distributed ledger or the smart contract be described in detail. The CMTA, however, recommends that issuers:

- provide general information about the consensus protocol used on the distributed ledger and the eligibility criteria for validators (i.e., whether the distributed ledger used is a public or a permissioned blockchain); if the relevant information is notorious or readily available from public sources, the information provided may cross-refer to such sources, which must in such a case be identified with specificity and retrievable from a non-alterable source;
- if the distributed ledger used is a permissioned blockchain, provide information about how the validators are selected and by whom;
- explain that the issuer may, one day, disable the tokens and decide to issue the Instruments in another form (including tokens recorded in a different distributed ledger);
- explain that the tokens are operated through a smart contract and give information about the tokens' key functions, in particular those that may give the issuer the power to freeze or disable tokens without the consent of the relevant token holder; and
- explain how any transfer restrictions are implemented (e.g., through a separate smart contract with specific functions).

Requirement

16: The Issuer provides each token holder with information regarding the functioning of both the distributed ledger and the smart contract used for the tokenization process (including the validation process, an explanation of the possibility for the Issuer to freeze or disable the tokens, and the tokens' key functions) as well as the technical and organizational measures to protect the functioning and integrity of the distributed ledger and the smart contract.

Recommendation

17: The information provided should include at a minimum:

- the type of persons eligible to validate entries in the distributed ledger and if the circle of validators is limited by the rules of the ledger (i.e., whether the distributed ledger used is a public or a permissioned blockchain);
- if the distributed ledger used is a permissioned blockchain, details about how the validators are selected and by whom;
- an indication that the issuer may, one day, disable the tokens and decide to issue the Instruments in another form (including tokens recorded in a different distributed ledger);
- an indication that the tokens are operated through a smart contract and give details about the tokens' key functions, in particular those that may give the Issuer the power to freeze or disable tokens without the consent of the relevant token holder; and
- indications as to the way any transfer restrictions contemplated in the terms and conditions of the Instruments are implemented.

§ 2.6 Valid issuance

The tokenization process relies on the due issuance of the Instruments associated with the digital tokens created by means of the smart contract. This in turn requires compliance with the legal requirements of the laws governing the issuer and the requirements of the issuer's constitutive documents.

Requirement

18: The issuer must have legal capacity and have validly resolved to issue the Instruments in the form of ledger-based securities pursuant to Article 973*d et seq.* CO (being all or a clearly identified portion of a particular issue).

Recommendation

19: A Swiss Issuer should resolve to issue the Instruments in the form of ledger-based securities substantially as outlined in Appendix 4. Issuers organized under laws other than Swiss law should adopt substantially similar resolutions.

§ 2.7 Deployment of the smart contract on the distributed ledger and allocation of the tokens to Instrument holders

To allocate the tokens to the Instrument holders for the first time, the issuer or its delegate must gather the holders' distributed ledger addresses (which can be ledger addresses controlled by the beneficial owner of the instrument itself, a nominee, or a custodian holding the tokens for the account of the holder). Once the distributed ledger addresses have been gathered, the tokens must be allocated to their holders. This can be done either manually or with the help of a dedicated smart contract (distinct from the smart contract used to create the tokenized Instruments), which automatically transfers a number of tokens corresponding to the number of Instruments held by each holder on the distributed ledger addresses provided by such holders.

Requirement

20: The issuer must have transferred the tokens associated with the digital Instruments to the distributed ledger addresses provided by the relevant holders.

3. POST-TOKENIZATION ACTIONS

§ 3.1 Identification of holders - Whitelisting features

Swiss and other laws against money laundering and the financing of terrorism require that financial intermediaries be in a position to identify both the person on whose behalf they may hold a particular Instrument in custody, and the intended recipient of such Instrument (unless the Instrument is to be transferred to another financial intermediary that is subject to adequate anti-money laundering regulations). Even if the Instruments are not held through a financial intermediary,

national and international embargo or sanction regimes may make it necessary for an issuer to identify the holders and beneficial owners of an Instrument before making any payment thereunder. Issuers may also wish to monitor who holds the Instruments they have issued for reputational or tax reasons (to the extent such restrictions are supported by the market on which the Instruments are traded, if applicable).

Issuers can generally use two methods to comply with applicable laws and manage legal and reputational risks in this context:

- ***Ex ante* control**. This method consists in issuing Instruments that, according to their terms and conditions, can only be validly transferred with the consent of the issuer[5]. In such a case, the legal title to the Instruments only passes to the acquirer when the transfer has been approved by the issuer, and the issuer only approves a transfer when it is satisfied that the acquirer is an eligible person. This control can be implemented in two ways:
  - an **ad hoc approval process** where each transfer requires the issuer's approval; or
  - a **whitelisting regime** where the issuer pre-approves transfers for a defined set of ledger addresses. The issuer can delegate the responsibility to allow or disallow ledger addresses to a third party service provider, as for example the operator of the platform on which the Instruments are traded, which will then allow the ledger addresses of its participants.
- ***Ex post* control.** This method consists in issuing freely transferable Instruments, but to restrict the ability of the acquirer to exercise the associated rights until the issuer has confirmed the acquirer's eligibility.

Issuers may choose any of these regimes under this Debt Standard. They must however ensure that the terms and conditions of the Instrument contemplate the whitelisting regime and that the relevant smart contract used for the tokenization of the Instruments is configured in accordance with the chosen regime. A critical requirement for ledger-based securities under Swiss law is that legal title to the Instrument follows the control over the relevant digital token. Therefore:

- If the issuer opts for an *ex ante*, ad hoc approval process (which will generally exclude the admission of the relevant Instrument to trading on a trading venue), the smart contract must be configured to allow transfers only with the issuer's approval. If the smart contract used is the CMTAT, this can be achieved by activating the "conditional transfer" rule of CMTAT's RuleEngine contract. If the issuer opts for a whitelisting regime and uses the CMTAT, it can use the Whitelist rule of the RuleEngine[6] to whitelist the relevant ledger addresses.
- If the issuer opts for an *ex post* control, it must make sure that the rights under the Instruments, although validly transferred with the relevant token, can only be exercised when the issuer has satisfied itself that the acquirer is an eligible person. This can be achieved by supplementing the terms and conditions of the Instruments to specify that token holders can only exercise their rights under the Instruments if they have identified themselves to the satisfaction of the issuer. An issuer wishing to avoid the efforts associated with identifying all token holders and their beneficial owners can decide to pre-approve addresses controlled by professional custodians subject to adequate regulations against money laundering and the financing of terrorism, and to limit *ex post* controls to holders that do not use such custodians. A specimen of supplemental terms for *ex post* controls is provided in Appendix 3.

5 See footnote 3 in Section 1.2.3 above on the compliance of such a regime with the requirement of Article 973d para. 2 No. 1 CO.

6 https://cmta.ch/standards/ruleengine-for-cmtat

If the issuer whitelists ledger addresses controlled by professional custodians and blocks the transfer to other addresses, the adoption of regulations for ex post controls is technically not necessary. However, issuers may still wish to adopt supplemental terms similar to those contemplated in Appendix 3 in such cases, to document the conditions under which professional custodians' ledger addresses will be whitelisted.

Requirement

21: Any restrictions to the transfer of Instruments contemplated by the terms and conditions of such Instruments must be duly reflected in the functionalities of the smart contract, so that the title to the relevant Instruments cannot be transferred without the relevant tokens and vice versa.

Recommendations

22: If the terms and conditions of the Instruments make their transfer subject to an ad hoc approval of the issuer, the issuer uses the CMTAT's "conditional transfer" feature, or an equivalent feature if using another smart contract recognized by CMTA. If the terms and conditions of the Instruments contemplate a whitelisting regime, the issuer uses CMTAT's RuleEngine smart contract to implement the relevant restrictions, or an equivalent feature if using another smart contract recognized by CMTA.

23: If the issuer chooses to implement *ex post* controls, the issuer adopts regulations substantially in the form contemplated in Appendix 3 to restrict the exercise of any right under the relevant Instrument until the identity of the token holder and, if different, of the Instrument's beneficial owner has been identified to the satisfaction of the issuer.

§ 3.2 Tokenized Instruments as intermediated securities

3.2.1 Principle

"Intermediated securities" within the meaning of the Federal Act on Intermediated Securities of 2008, as amended (the "**FISA**") can be created with tokenized Instruments. For this purpose, the tokenized Instruments have to be transferred to a professional custodian (e.g., a bank, a securities firm, a DLT-based trading facility or a central securities depository (CSD) within the meaning of the Financial Market Infrastructures Act) and subsequently credited (as book-entry securities) on a securities account in the name of the relevant holder, maintained by the respective custodian.

3.2.2 Transfers of tokenized Instruments held on a securities account

Once tokenized Instruments are credited on a securities account held with a custodian, the tokenized Instruments can be transferred or encumbered in the manner contemplated by the FISA if the relevant custodians are located in Switzerland, i.e., through the debit and credit of the securities accounts of the transferor and transferee (Article 24 FISA), or through the execution of a so-called "control agreement" with the relevant custodian (Article 25 FISA). In such a case, the transfer of ownership does not require the transfer of the relevant token.

§ 3.3 Switch to non-tokenized Instruments or to new tokens

The decision to tokenize Instruments is not irreversible. Reversing such a decision may even be necessary in the event of a temporary or permanent malfunction or unavailability of the relevant distributed ledger or of the smart contract that governs the tokens (e.g., in the event of hack, governmental intervention or network congestion).

The process to de-couple Instruments from the digital tokens with which they are associated is similar to the one by which an issuer cancels certificated securities that have been surrendered to it. In such a case, the terms and conditions of the Instruments may offer several options to the issuer: issuing new digital tokens (e.g., on a different distributed ledger), keeping the Instruments in uncertificated form without tokenizing them, or issuing physical (individual or global) certificates representing the Instruments.

From a technical perspective, the cancellation of tokens can be achieved by using the issuer-only "deactivateContract" function of the CMTAT smart contract. This function permanently and irreversibly deactivates the smart contract (unless a proxy is used), but does not affect the record of past transactions in the distributed ledger. At the same time, the Instruments will have to be de-coupled from the tokens.

Although the Instruments formerly associated with the cancelled tokens can no longer be transferred on the distributed ledger, the last entries recorded before the token was cancelled are evidence of the holders' legal title to the relevant Instruments. These entries can consequently be used to identify the persons to whom new tokens or certificates must be delivered.

If the cancellation relates to some tokens only (but not all of them), the operation can be carried out by using the "Burn" function of the smart contract).

§ 3.4 Corporate actions

Corporate actions, such as interest payments or redemption, cannot be carried out automatically unless specific functions have been created to that effect in the smart contract that governs the tokens. Such actions require either a separate payment or transfer carried out off-chain or a cancellation of the existing tokens and the allocation of new tokens to the distributed ledger address of the former holders.

§ 3.5 Cancellation of tokens when the relevant private key has been lost or stolen

Swiss law contemplates a specific provision to address situations in which the private key of a particular token has been lost or stolen. Similarly to what is contemplated in case of loss or theft of certificated securities, Article 973*h* CO allows the court to cancel a token if the person controlling a given private key has not responded to notices published in the Swiss Official Gazette of Commerce. As mentioned above (see § 2.3 above), when tokenized Instruments are issued under this Debt Standard, jurisdiction for the cancellation of a token must be given to a Swiss court.

Upon production of an enforceable court decision, the token holder whose private key has been lost or stolen can ask the issuer to cancel the relevant token and to issue a new one to the distributed ledger address of its choice.

To simplify the measures that must be taken in the event of loss or theft of private keys, CMTA recommends that, in accordance with Article 973*h* para. 2 CO, the number of public notices required as part of the cancellation process be reduced to one and that the deadline imposed on token holders to produce the relevant private keys be reduced to one month.

Recommendation

24: The tokenization terms applicable to the tokenized Instruments provide that, if court proceedings are initiated pursuant to Article 973*h* CO to cancel tokens for which the private key has been lost or stolen, the number of public notices required is reduced to one and the deadline imposed on token holders to produce the relevant private keys is reduced to one month.

This standard was adopted on May 19, 2025.

Capital Markets and Technology Association

cmta.ch

Route de Chêne 30
1208 Geneva

admin@cmta.ch

APPENDIX 1: CMTA TEMPLATE TOKENIZATION TERMS AND INFORMATION DOCUMENT

Tokenization terms of [name of the company]

1. SCOPE AND PURPOSE

This document is an appendix to, and incorporated by reference in, the terms and conditions (the "**Terms and Conditions**") of certain securities (the "**Securities**") issued by the issuer identified in the Terms and Conditions (the "**Issuer**"). It contains (i) the tokenization terms (*Registrierungsvereinbarung / convention d'inscription*) within the meaning of Articles 973*d* and 973*f* of the Swiss Code of Obligations in respect of such Securities and (ii) general information on the tokenization process of securities and distributed ledgers.

2. ASSOCIATION OF THE SECURITIES WITH DIGITAL TOKENS RECORDED IN A DISTRIBUTED LEDGER

The Securities have been or will be issued in the form of ledger-based securities within the meaning of Article 973*d* of the Swiss Code of Obligations ("**Ledger-Based Securities**").

Each Ledger-Based Security is or will be associated with a digital token (each a "**Token**") recorded in a distributed ledger (the "**Distributed Ledger**") identified in the Terms and Conditions. The creation of and operations on the Tokens shall take place within the technical framework of one or several smart contracts identified below (collectively, the "**Smart Contract**"). The Tokens are – from a technical standpoint – entries in a sub-ledger maintained in the Distributed Ledger by means of the Smart Contract.

For the purpose of these tokenization terms, the Smart Contract shall be [the open-source computer code framework "CMTAT" applicable to the Distributed Ledger, as published on the website of the Capital Markets and Technology Association (see Section 7.3 below)].

Each of the Distributed Ledger and the Smart Contract used for the creation of the Ledger-Based Securities is identified in the Terms and Conditions. The Ledger Address (as defined below) of the Smart Contract is also indicated in the Terms and Conditions. The computer code of the Smart Contract contains (i) a URL to these tokenization terms and information document, and (ii) a unique identifier that is tied to the Terms and Conditions (the "**Unique Identifier**"). The Unique Identifier serves as evidence that a specified Token has been associated with a specified Security. [The Unique Identifier will generally take the form of a series of hexadecimal characters found both in the computer code of the Smart Contract and in the digital signature of the document containing the Terms and Conditions.]

3. TRANSACTIONS IN LEDGER-BASED SECURITIES

3.1 Transfer of title and creation of interests on Ledger-Based Securities

Subject to any other methods of transfer permitted by law and any transfer by operation of law (e.g., in the event of universal succession further to the death or merger of the Security holder, or if a transfer or encumbrance is carried out pursuant to rules applicable to intermediated securities), the transfer of legal title to the Ledger-Based Securities and the creation of a security or other interest (such as a pledge or other security interest) on such Ledger-Based Securities (each such transfer or creation of interest a "**Transaction**") shall require the recording of the transfer of the relevant Token on a Ledger Address controlled by the acquirer, in accordance with the rules and procedures of the Distributed Ledger and the functions of the Smart Contract.

A Token transfer will be deemed to have been recorded in the Distributed Ledger when [30 blocks or more have been validated after the one relating to the relevant Transaction]. If the Ledger-Based Securities are traded on a trading platform the record of a transfer may be subject to the validation of the number of blocks specified by the rules of the relevant trading platform.

Once a Transaction has been recorded in the Distributed Ledger, the Transaction will remain valid if the agreement based on which the Transaction was carried out is invalidated (for example as a result of a fraud or material error of one of the parties). In such a case, the unwinding of the Transaction shall require a return of the relevant Token to a Ledger Address controlled by the transferor.

3.2 Transfer restrictions

Notwithstanding Section 3.1:

a. if the Terms and Conditions provide that the Securities can only be transferred with the prior consent of the Issuer, the Smart Contract will only permit Tokens to be transferred with the approval of the Issuer or its authorized representative, and no Security holder shall have a right to have the Tokens that it controls transferred without the consent of the Issuer; and

b. if the Terms and Conditions provide that the Ledger-Based Securities can only be transferred to Ledger Addresses that have been approved by or on behalf of the Issuer (a "**White Listed Address**"), the Smart Contract will only permit Tokens to be transferred to White Listed Addresses, and no Security holder shall have a right to have the Ledger-Based Securities that it holds transferred to a Ledger Address that is not a White Listed Address.

4. HARD FORKS

In this Section 4, "**Hard Fork**" means a disagreement among participants of the Distributed Ledger resulting in a split into two or more incompatible versions of such Distributed Ledger, and which results in the Tokens recorded in the Distributed Ledger being duplicated (one version of the Tokens remaining on each version of the Distributed Ledger).

In the event of a Hard Fork or under similar circumstances that may endanger the reliability of the Distributed Ledger, the Issuer may activate the "pause" function of the Smart Contract to prevent Transactions on both versions of the Distributed Ledger pending its decision on which version it will support and the communication of such decision to the Security holders.

If the Issuer decides to support the version of the Distributed Ledger that follows the rules and protocols of such Distributed Ledger that were in force immediately prior to the occurrence of the Hard Fork (i.e., the "legacy" version of the Distributed Ledger), all Transactions on "forked" versions of the Distributed Ledger will be invalid, and any Token existing on a forked version of the Distributed Ledger will not be associated with any Security. If the Issuer decides to support a forked version of the Distributed Ledger, all Transactions on the "legacy" version of the relevant Distributed Ledger will be invalid, and any Token existing on the "legacy" version of the Distributed Ledger will not be associated with any Security.

If the Issuer does not activate the "pause" function and does not indicate which version of the Distributed Ledger it chooses, the Issuer shall be deemed to have chosen to support the version of the Distributed Ledger that is the most commonly used among industry participants (which will in principle be the version which has the highest number of validators and active users).

5. CANCELLATION OF LOST OR STOLEN TOKENS

If a holder of Ledger-Based Securities initiates proceedings to have one or more Tokens cancelled pursuant to Article 973*h* of the Swiss Code of Obligations, the number of public notices required pursuant to Article 973*h* para. 2 of the Swiss Code of Obligations will be one, and the deadline

imposed on Token holders to produce the relevant private keys will be one month. The Issuer will cancel and re-issue a Token upon delivery of an enforceable (*vollstreckbar*, *exécutoire*) court decision ordering such cancellation and re-issue.

6. AMENDMENTS

The Issuer may amend these tokenization terms at any time and without prior notice. Amendments to these tokenization terms will be validly made and binding upon all Security holders once published in accordance with the Terms and Conditions. Amendments to these tokenization terms will only affect the acquisition, encumbrance or disposal of Securities (including Transactions) entered into after the amendments became effective and will not affect such transactions (including Transactions) previously completed.

7. ADDITIONAL INFORMATION REGARDING THE LEDGER-BASED SECURITIES, THE DISTRIBUTED LEDGER AND THE SMART CONTRACT

7.1 Functioning of the Distributed Ledger and the Smart Contract

The distributed ledger technology is a technology that allows the operation of a distributed ledger, i.e., a ledger that is not kept by a trusted intermediary but by a community of independent participants.

The distributed ledger technology, as implemented on the Distributed Ledger is based on complex mathematical and cryptography concepts, which are described in this document at a high level only. The technology makes it possible to keep records of data relating to persons whose identity is protected by asymmetric cryptographic methods. Such methods are based on the interplay between a public key and a private key, which are two numbers that are mathematically related. The public key, often referred to as the "distributed ledger address" (the "**Ledger Address**") is available to all ledger participants, while the private key must remain secret.

The holder of the private key can generate "signature messages" that can be identified as authentic (i.e., as having been generated with the private key) by the ledger participants. Such signature messages can be used to initiate "transactions", i.e., new entries in the ledger. In a distributed ledger that functions as a "blockchain", the participants validate transactions in blocks, by adding a new set of data (or "block") to a chain of pre-existing blocks. Each ledger participant maintains its own copy of the ledger, and updates such copy when a participant includes a new "block" in a manner consistent with the chain's protocol. This regime aims to ensure the transparency and immutability of the transactions recorded in the ledger.

7.2 Information on the functioning of the Distributed Ledger

If the Terms and Conditions designate "[the Ethereum Blockchain]" as the Distributed Ledger with respect to the Ledger-Based Securities, the Tokens will be recorded on the [Ethereum] distributed ledger.

[The Ethereum distributed ledger has two functions:

- The first is related to Ether (or ETH). Ether is a cryptocurrency (or digital currency) that is recorded and traded on the distributed ledger. Users of the Ethereum distributed ledger can trade Ethers on the distributed ledger and use Ethers as a means of payment or to access functions of the Ethereum distributed ledger.
- The second is the use of smart contracts. The Ethereum distributed ledger allows for the creation of computer codes called "smart contracts", which can perform a large number of functions, including creating a record of digital tokens on ledger addresses. A "token" is an entry in a register that is maintained by means of a smart contract. Each token is attributed to a particular ledger address. The fact that the register maintained through the

smart contract contains a corresponding entry is evidence that a token is attributed to the relevant ledger address. Entries in the distributed ledger are validated by a large number of participants. Any person or entity may act as validator and validate transactions in the distributed ledger, subject to technical requirements unrelated to the identity of the person or entity (e.g., technical infrastructure requirements and / or minimum amount of Ethers "staked", i.e., locked on a ledger address for a certain period of time).]

7.3 Information on the CMTAT smart contract framework

The Ledger-Based Securities are created and managed by means of the CMTAT, an open-source computer code framework published by the Capital Markets and Technology Association (the "**smart contract**")[1]. The smart contract defines the manner in which the Tokens are created, transferred and cancelled. The smart contract also serves to record the ownership of the Tokens.

[For Ethereum:]

The [Solidity] source code and the distributed ledger address of the smart contract are published at [https://etherscan.io/token/[•]].

The code of the CMTAT has been released under Mozilla Public License 2.0. Under the terms of that license, the code is provided on an "as is" basis, without warranty of any kind including warranties that the code is free of defects, merchantable, fit for a particular purpose or non-infringing.

8. GOVERNING LAW AND JURISDICTION

All matters addressed in these tokenization terms (*Registrierungsvereinbarung / convention d'inscription*) are governed by Swiss law, excluding any application of private international law rules. The law applicable to the Securities, as set out in the Terms and Conditions, is not affected by these tokenization terms.

Without affecting the right of any Security holder to bring a dispute related to a Security to the courts having jurisdiction under the laws applicable to the Securities, as set out in the Terms and Conditions the courts of [the canton of [•] in Switzerland], shall have jurisdiction (a) over disputes concerning the acquisition, encumbrance or disposal of Securities (including the validity of Transactions carried out on the Distributed Ledger), the issuance of the Securities in the form of, and the form of, Ledger-Based Securities, and the termination of the regime applicable to Ledger-Based Securities to some or all of the Securities, and (b) for the cancellation of Tokens pursuant to Article 973*h* of the Swiss Code of Obligations and Section 5 of these tokenization terms.

---

1 Alternative provision: "The Ledger-Based Securities are created and managed by means of a smart contract (the "**smart contract**") that has been approved by the Capital Markets and Technology Association for that purpose.

APPENDIX 2: MAIN FEATURES OF A SMART CONTRACT FOR THE TOKENIZATION OF INSTRUMENTS

1. MAIN FEATURES OF A SMART CONTRACT FOR THE TOKENIZATION OF INSTRUMENTS

A smart contract used for the tokenization of Instruments under this Debt Standard (such as the open source smart contract "CMTAT" published by the CMTA) must have the following characteristics.

(a) Basic parameters of the token

To facilitate the token's use on wallets and trading platforms, the token should be given:

- a **name** that has preferably not been used for another token or another publicly traded security;
- a reference to (e.g. in the form of an Internet address) or a hash of the **tokenization terms and the information required by law** about the distributed ledger and the smart contract (see 2.4.3 of this standard); and
- a **ticker symbol**.

(b) No fractions

The smart contract must define the tokens so that they can only represent whole numbers (as opposed to real numbers). Further, tokens must have a decimal place set to zero (meaning that the transfer of a fraction of a token is not possible).

(c) Transfers

The smart contract must allow holders to transfer tokens from one distributed ledger address that they control to another distributed ledger address that they do not necessarily control.

(d) Mint (issuer function)

The issuer must be in a position to create new tokens by allocating new tokens to a distributed ledger address.

This function is meant to be used when the issuer tokenizes newly issued Instruments or existing Instruments previously issued in a different form (e.g. in the form of individual or global certificates).

(e) Burn (issuer function)

This function allows the issuer to destroy specific tokens that are recorded on a distributed ledger address.

This function is meant to be used if the issuer cancels tokenized Instruments (e.g. if it retires Instruments or decides to have the Instruments in a different form (e.g. "simple" uncertificated securities within the meaning of Article 973*c* CO or paper certificates), or to comply with a court order requiring the cancellation of tokens pursuant to Article 973*h* CO).

(f) Pause (issuer function)

The issuer must be able to "pause" the smart contract, to prevent execution of transactions on the distributed ledger until the issuer puts an end to the pause. This function can be used to block transactions in case of a "hard fork" of the distributed ledger, pending a decision of the issuer as to which version of the distributed ledger it will support.

(g) Address Freeze (issuer function)

The issuer (or a third party appointed by it) must be in a position to freeze tokens on specific distributed ledger addresses (as opposed to pausing the whole smart contract) to prevent the transfer of tokens that have been earmarked for transfer to a third party (e.g. between the execution of a transaction on a trading platform and the settlement of the trade in the distributed ledger).

(h) "deactivate Contract" (issuer function)

Contrary to the "burn" function mentioned under (e) above, the "deactivateContract" function affects all tokens in issue, and not only some of them. This function is necessary to allow the issuer to carry out certain corporate actions (e.g. share splits, reverse splits or mergers), which require that all existing tokens are either cancelled or immobilized and decoupled from the Instruments (i.e. the tokens no longer represent Instruments).

The "deactivateContract" function can also be used if the issuer decides that it no longer wishes to have the Instruments issued in the form of ledger-based securities within the meaning of Article 973*d* CO, but rather as "simple" uncertificated securities within the meaning of Article 973*c* CO or of certificated securities. The "deactivateContract" function does not delete the contract's storage and code, i.e. tokens are not burned by the function, however it permanently and irreversibly deactivates the smart contract (unless a proxy is used). In such cases, the last entries in the distributed ledger make it possible to identify the last owners of the Instruments.

2. INFORMATION ABOUT INSTRUMENTS

In addition, the smart contract should include information about the Instruments that are being tokenized. It is recommended that the required information should cover all applicable fields in the most recent Bond Data Taxonomy published by the International Capital Market Association (ICMA); the issuer should ensure that full text, hash or a unique identifier of the terms and conditions is included.

Alternatively, the smart contract should include the following information about the Instruments being tokenized:

1. *Information on the issuer and other persons involved*
   - (i) Issuer identifier (legal entity identifier [LEI] or, if unavailable, Swiss entity identification number [UID] or equivalent)
   - (ii) Guarantor identifier (legal entity identifier [LEI] or, if unavailable, Swiss entity identification number [UID] or equivalent), if applicable
   - (iii) Debtholders representative identifier (legal entity identifier [LEI] or, if unavailable, Swiss entity identification number [UID] or equivalent), if applicable
2. *Information on the Instruments*
   - (i) Unique identifier / hash, if applicable
   - (ii) Issuance date
   - (iii) Currency of payments, if applicable
   - (iv) Par value (aggregate principal amount), if applicable
   - (v) Minimum denomination, if applicable

(vi) Maturity date, if applicable

(vii) Interest rate, if applicable

(viii) Coupon payment frequency, if applicable

(ix) Interest schedule format, if applicable. The purpose of the interest schedule is to set, within the parameters of the smart contract, the dates on which the interest payments accrue.

- Format A: start date/end date/period
- Format B: start date/end date/day of period (e.g., quarter or year)
- Format C: date 1/date 2/date 3/….

(x) Interest payment date (if different from the date on which the interest payment accrues):

- Format A: period (indicating the period between the accrual date for the interest payment and the date on which the payment is scheduled to be made)
- Format B: specific date

(xi) Day count convention

(xii) Business day convention

APPENDIX 3: ADDITIONAL TERMS FOR *EX POST* CONTROLS – REGISTER OF HOLDERS

Issuers that perform *ex ante* controls may adopt regulations regarding procedures to follow to grant ad hoc approvals or whitelisting, as applicable. Those should match the terms and conditions of the Instruments and be consistent with the Debt Standard.

Issuers that do not perform *ex ante* controls over the identity of the acquirers of tokens are recommended to maintain a register of the persons who do not hold their Instruments via a professional custodian that is subject to adequate regulations against money laundering and the financing of terrorism, and to adopt regulations for the maintaining of such register of holders essentially as set forth below.

Regulations of [name of the company] regarding the maintenance of the register of holders of [description of the Instruments]

1. SCOPE AND PURPOSE

This document defines the rules and procedures for the creation and maintenance of a register of holders (the "**Register of Holders**") of [designation of the tokenized instruments] (the "**Securities**") issued by [name of the Issuer] (the "**Issuer**"). It supplements the terms and conditions of the Securities, as well as their tokenization terms (*Registrierungsvereinbarung / convention d'inscription*) within the meaning of Articles 973*d* and 973*f* of the Swiss Code of Obligations.

These regulations only apply as long as the Securities are issued in the form of ledger-based financial instruments within the meaning of Articles 973*d et seq.* of the Swiss Code of Obligations.

Only Sections 2 and 3 of these regulations apply if the smart contract that has been used to generate the digital tokens associated with the Securities (the "**Tokens**") prevents the holders of such Securities (each a "**Holder**") from transferring the Tokens to ledger addresses that are not controlled by professional custodians within the meaning of the Swiss Federal Act on Intermediated Securities of 2008, as amended (e.g., banks, securities firms, DLT-based trading facilities or central securities depositories within the meaning of the Financial Market Infrastructure Act of 2015, as amended) (a "**Regulated Custodian**").

2. REGISTER OF HOLDERS

The Company maintains a Register of Holders in accordance with these regulations. It can delegate the maintenance of such Register of Holders to a third party.

A registration of a transfer in the distributed ledger on which the Tokens are recorded, or a "whitelisting" of a ledger address in a rule engine associated with the smart contract used for the tokenization of the Securities (the "**Smart Contract**") will be deemed a registration in the Register of Holders for the purpose of these regulations.

3. REQUIREMENTS FOR REGULATED CUSTODIANS

Acquirers of Tokens that are Regulated Custodians can be recorded in the Register of Holders if they provide the following information:

(i) Name, address and legal entity identifier ("**LEI**") of the Regulated Custodian;

(ii) distributed ledger address(es) on which the Securities are to be recorded;

(iii) confirmation that the Regulated Custodian controls the ledger address(es) referred to under (ii) above; and

(iv) if applicable, the fact that the Securities held by the Regulated Custodian are held on an omnibus distributed ledger address (i.e., on a distributed ledger address that is maintained for multiple beneficial owners).

4. RESTRICTION IN THE RIGHTS OF UNREGISTERED HOLDERS

If the terms and conditions of the Securities provide that the Securities can only be transferred with the prior approval of the Issuer (and that the Smart Contract consequently only permits the transfer of Tokens on ledger addresses approved by the Issuer), the legal title to the Securities and the rights thereunder will be subject to the registration of the Tokens on a ledger address controlled by the acquirer, in accordance with the tokenization terms.

If the Securities are freely transferable under their terms and the Tokens can consequently be transferred to any ledger address, the exercise of the rights under the relevant Securities (including the right to the payment of principal or interest, or of option, conversion or other rights) will be suspended until the Holder is registered in the Register of Holders.

To be registered in the Register of Holders, acquirers of Securities must follow the rules and procedures contemplated in these regulations.

5. REGISTRATION REQUESTS

To be registered in the Register of Holders, acquirers of Securities other than Regulated Custodians must submit a duly completed registration request in the manner contemplated in these regulations. The Issuer may refuse to register an acquirer of Securities in its Register of Holders if it determines in good faith that doing so would infringe applicable laws, including but not limited to laws on embargoes or implementing international sanctions.

The Issuer may, at its discretion, register acquirers of Securities in its Register of Holders if it has otherwise satisfied itself that the identity of such acquirers has been sufficiently determined, and that such registration is consistent with applicable laws.

5.1 Form of the registration request

Registration requests must be made in writing to the following address [•] or by such other means as may be communicated by the Issuer.

5.2 Content of the request – Securities acquired by the beneficial owner

Holders other than Regulated Custodians must provide the following information:

(i) first and last name (for individuals) or corporate name (for legal entities and unincorporated partnerships) and LEI (if available) of the applicant;

(ii) details of the applicant:

- place of residence (for individuals) or registered office (for legal entities and unincorporated partnerships) and valid postal address;
- date of birth (for individuals) or date of constitution (for legal entities and unincorporated partnerships);
- nationality(ies) (for individuals);
- email address;
- telephone number;

- copy of a document used to verify the identity;

(iii) confirmation that the applicant holds the Securities for its own account and not for the benefit of a third party;

(iv) IBAN of a bank account opened in the name of the applicant with a bank established in Switzerland or in another member State of the Organization for Economic Co-operation and Development (OECD);

(v) distributed ledger address(es) on which the Securities are to be recorded; and

(vi) confirmation that the applicant has sole control over the distributed ledger address(es) referred to under (v) above.

5.3 Content of the request – Securities acquired through a fiduciary

All persons and entities who have acquired Securities through a third party (fiduciary) that is not a Regulated Custodian must themselves or through the fiduciary provide the following information:

(i) first and last name (for individuals) or corporate name (for legal entities and unincorporated partnerships) and LEI (if available) of the beneficial owner;

(ii) details of the beneficial owner:

- place of residence (for individuals) or registered office (for legal entities and unincorporated partnerships) and valid postal address;
- date of birth (for individuals) or date of constitution (for legal entities and unincorporated partnerships);
- nationality(ies) (for individuals);
- email address;
- telephone number;
- copy of a document used to verify the identity;

(iii) name and address of the fiduciary;

(iv) confirmation from the fiduciary that the identified beneficial owner beneficially owns the relevant Securities;

(v) IBAN of a bank account opened in the name of the fiduciary with a bank established in Switzerland or in another member State of the Organization for Economic Co-operation and Development (OECD);

(vi) distributed ledger address(es) on which the Securities are to be recorded;

(vii) confirmation from the fiduciary that the fiduciary controls the ledger address(es) referred to under (vi) above; and

(viii) if applicable, the fact that the Securities acquired by the fiduciary for the beneficial owner are held on an omnibus distributed ledger address (i.e., on a distributed ledger address that is maintained for multiple beneficial owners).

6. GENERAL PROVISIONS

6.1 Supporting evidence

The Issuer may request supporting evidence in relation to a registration.

The Issuer may in particular request that a beneficial owner or fiduciary acting on behalf of a beneficial owner performs a so-called “satoshi test”, i.e., makes a small transaction from

the distributed ledger address purported to be the applicant's, or otherwise request that the respective beneficial owner or fiduciary demonstrates that it has control over the distributed ledger address on which the Tokens are recorded.

6.2 New confirmation

The Issuer may, at any time, request a Holder or Regulated Custodian to confirm that the information provided or the representations made to the Company as part of the registration process remain accurate and up to date.

6.3 De-registration

The Issuer may strike off the registration of any Holder or Regulated Custodian from the Register of Holders if it determines that the relevant registration was obtained on the basis of false or misleading information or representations, or if a Holder or Regulated Custodian fails upon request to confirm that the information provided or the representations made to the Issuer as part of the registration process remain accurate and up to date.

APPENDIX 4: RESOLUTIONS FOR THE TOKENIZATION OF SECURITIES

The specimens below only relate to the resolutions that the competent corporate body of an Issuer (e.g., its board of directors) needs to adopt to have the Instruments validly issued in the form of ledger-based securities pursuant to Articles 973*d et seq.* of the Swiss Code of Obligations. Those specimens do not cover other points that may have to be approved in connection with the issuance of the Instruments (e.g., approval of various transaction documents, issuance prospectus, or application to have the Instruments admitted to trading on a trading platform).

The [name of the relevant corporate body] of the Issuer resolves what follows:

1. The issuance of [name of the debt instrument], with the terms set forth in [name of the document containing the terms of the Instruments] (the "**Securities**"), in such numbers and to such initial investors as set out in Appendix [1] to these resolutions, is hereby approved.
2. The Securities will be initially issued in the form of ledger-based securities within the meaning of Article 973*d et seq.* of the Swiss Code of Obligations, and will be associated with digital tokens (each a "**Token**") recorded in the [Ethereum] distributed ledger (the "**Distributed Ledger**"), using the CMTAT smart contract in its version [•] dated [date], as published by the Capital Markets and Technology Association (the "**Smart Contract**")[2].
3. The Issuer's regulations attached as Appendix [2] to these resolutions, which (i) contain the information that the Issuer is required to provide under article 973i para. 1 of the Swiss Code of Obligations and (ii) set forth the tokenization terms of the Securities ("*Registrierungsvereinbarung*", "*convention d'inscription*") for the purpose of Article 973*d* para. 1 No. 3 and Article 973*f* para. 1 of the Swiss Code of Obligations (the "**Tokenization Terms**"), are hereby approved and adopted with immediate effect.
4. [The executive management] is hereby authorized and instructed to (i) take actions to deploy the Smart Contract on the Distributed Ledger and (ii) transfer Tokens created by means of the Smart Contract and evidencing the Securities on the ledger address(es) provided by the initial acquirer(s) of such Securities, including by mandating such service provider as [the executive management] may in its reasonable judgement consider necessary, appropriate or useful to carry out such tasks and by paying the corresponding fees, expenses or other amounts due to such service provider for such service.
5. [The executive management] is hereby authorized and instructed to procure that the Smart Contract is configured in such a manner that [the transfer of the Tokens is subject to a prior approval by the Issuer / Tokens can only be transferred to ledger addresses that have been approved by the Issuer][3].
6. [The Issuer shall maintain a register of holders of the Securities, in accordance with the regulations attached as Appendix [3] to these resolutions, which are hereby approved and adopted with immediate effect][4].
7. [Each member of the executive management] is hereby authorized and instructed to take such actions and execute such documents as may be necessary, appropriate or useful to give

---

2 Alternative provision: "The Securities will be represented by digital tokens (each a "**Token**") recorded in the [Ethereum] distributed ledger (the "**Distributed Ledger**") using a smart contract that has been approved by the Capital Markets and Technology Association (the "**Smart Contract**").

3 Only if the terms of the Securities contain corresponding restrictions to the transfer of the Securities.

4 Not necessary if the terms of the Securities make their transfer subject to an ad hoc prior approval of the Issuer.

effect to these resolutions.

Capital Markets and Technology Association

cmta.ch

Route de Chêne 30
1208 Geneva

admin@cmta.ch