SmartOne STANDARD 5000

First Edition
2019-01

Token Generation Event Standard - Overview and Vocabulary

Contents

Foreword

SmartOne is established as a Foundation with the intention of serving both as a provider of legal services to Token Generating Event organizers and financial institutions, and as an umbrella organization for the promotion of research, development and creation of standards to serve the wider legal and regulatory landscapes of the crypto community.

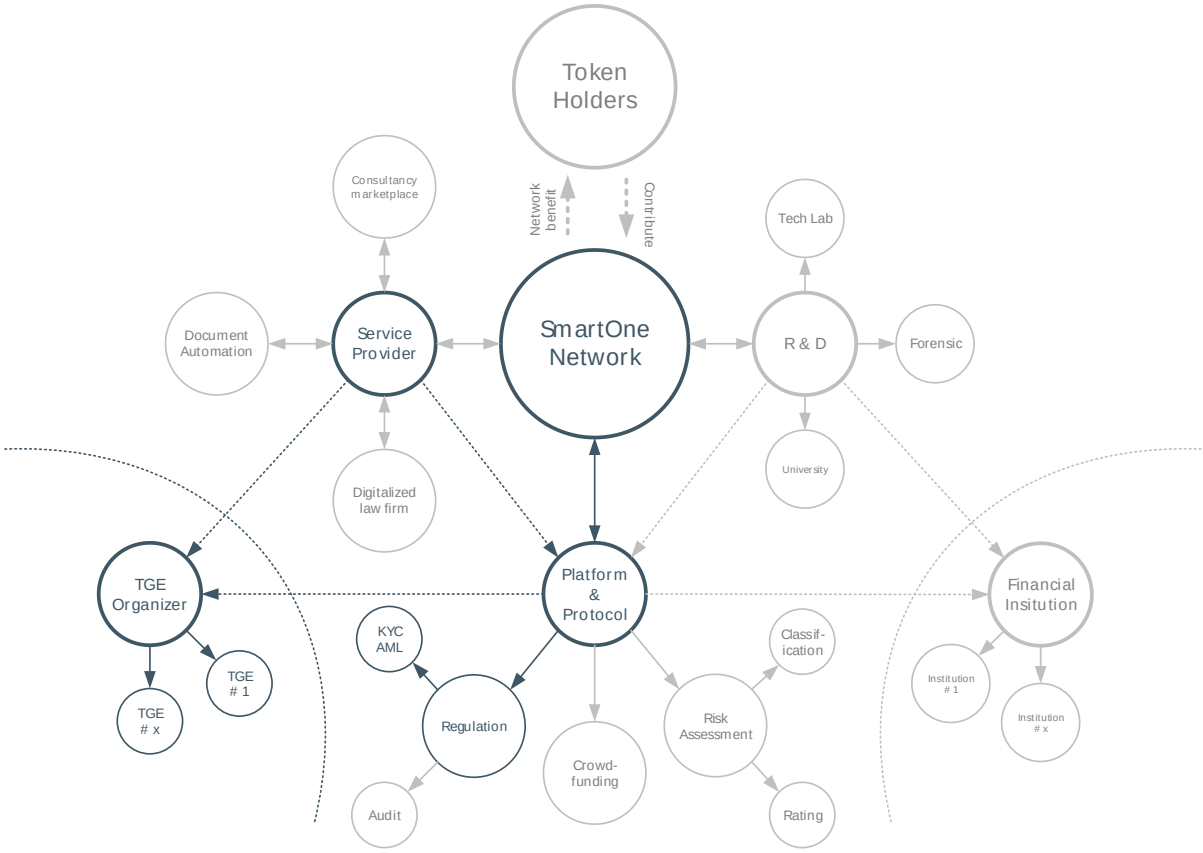
Attention is drawn to the possibility that some elements of this document may be subject of patent rights. SmartOne shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

Introduction

1 Overview

The SmartOne Foundation aims to provide and develop new technologies and applications focusing, in particular, on open and decentralised software architectures.



Over the last few years, blockchain technology has been receiving significant attention from investors, corporations and entrepreneurs. Unlike more traditional business transformations such as IPO's, the TGE space is immature with little context given to a regulatory or legal framework in which to operate.

This Standard forms part of the SmartOne protocol. The protocol is a family of Standards designed to position organizations wishing to undertake an TGE to meet or exceed high regulatory requirements. By adopting the methods and controls detailed in the series of Standards, organizations can legitimately demonstrate to investors and users alike its commitment to a more mature operating model. Furthermore, it prepares an organization to a level that can be independently assessed, promoting the status and credibility of an TGE.

The SmartOne Foundation maintains an expert committee dedicated to the development of TGE standards.

1.1 Using the Standards

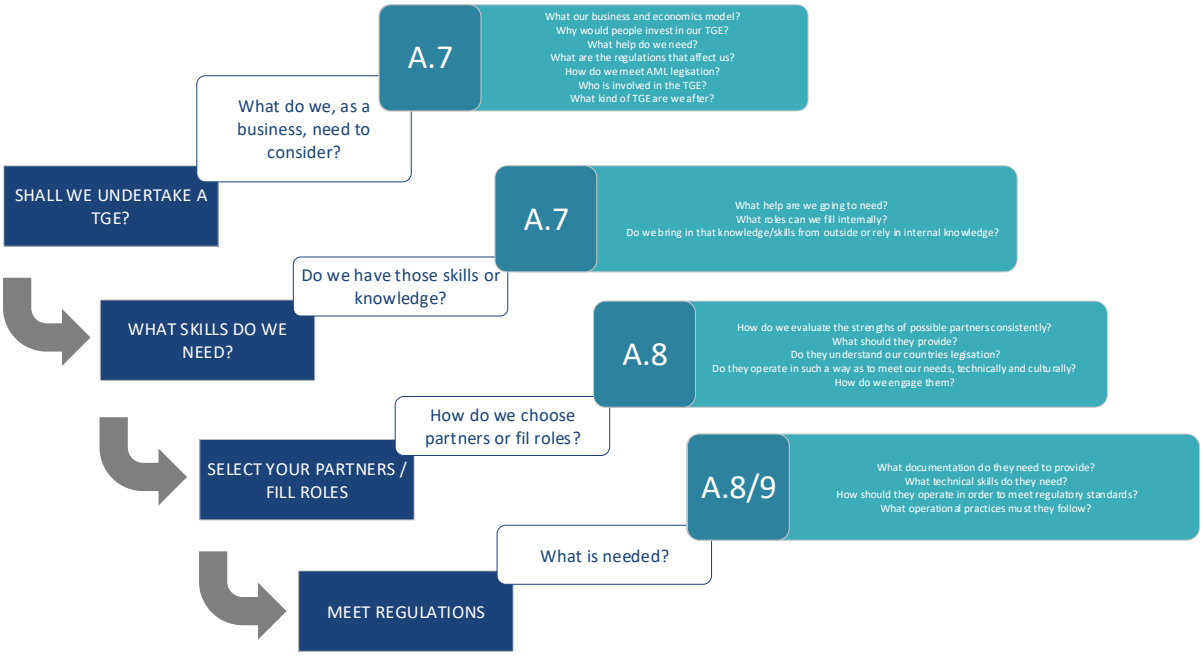
So you want to do a Token Generation Event (TGE)? And you want to carry out the TGE in the most efficient manner, utilizing best practice in the field and meet regulatory requirements for your country? You perhaps recognize that you need some help from external entities or want maybe you want to utilize your internal workforce but want to ensure that you have sufficient skills in house.

The SmartONE Standards are designed to help you accomplish that.

Two key questions can be answered:

- What steps do you need to do to achieve your TGE within a regulated environment?
- How to assess the skills you already have and those any partners have in a consistent manner?

The Standards provide a framework upon which to undertake a TGE to ensure you are ready as a business, you have the right skill sets and your choice of partners is sound. For example, does your legal role or partner understand the specific requirements for your country? Are you getting what you think you are getting from any technical role or partner?



The Standard itself is contained with 5001. In Annex A is lists out what you should be judged on by any future audit, what you should be judging others on and what you need to do.

5002 then breaks down each requirement into a set of specific controls. Not all controls will be mandatory. Some may be fundamental to meeting a regulated TGE, others may have complementing controls.

5000 – this document – explains any terms found in the Standards and the documents that form the Standard.

2 Scope

This document provides the overview of the TGE process. It also provides terms and definitions commonly used in the SmartOne family of Standards.

2.1 SmartOne Family of Standards

The SmartOne family of standards is intended to assist organizations of all types and sizes to implement a TGE and consists of the following Standards:

- SmartOne 5000, Token Generation Event Standard – Overview and vocabulary
- SmartOne 5001, Token Generation Event Standard – Requirements
- SmartOne 5002, Token Generation Event Standard – Code of practice controls
- SmartOne 5004, Token Generation Event Standard – Risk management
- SmartOne 5005, Token Generation Event Standard – Requirements for bodies providing audit and certification of TGE
- SmartOne 5007, Token Generation Event Standard – Guidelines for TGE systems auditing
- SmartOne 5008, Token Generation Event Standard – Guidelines for TGE security
- SmartOne 5009, Token Generation Event Standard – Specific guidelines for sectors/regions (Reserved)

2.2 General information

The TGE family of Standards consists of inter-related standards.

2.3 Standards describing an overview and terminology

2.3.1 SmartOne 5000 (this document)

Title: Token Generation Event Standard – Overview and vocabulary

Scope: This Standard provides to organizations and individuals:

- An overview of the TGE family of standards
- An introduction to TGE system
- Terms and definitions used throughout the TGE family of standards

Purpose: SmartOne 5000 describes the fundamentals of the TGE system which form the subject of the TGE family of standards and defines related terms.

2.4 Standards specifying requirements

2.4.1 SmartOne 5001

Title: Token Generation Event Standard – Requirements

Scope: This standard specifies the requirements for establishing and implementing a formalised TGE. It specifies requirements for the TGE controls customised to the needs of individual organizations or parts thereof. This Standard can be used by all organizations, regardless of type, size and nature.

Purpose: SmartOne 5001 provides normative requirements for the development and implementation of a TGE, including a set of controls for the control and mitigation of risks associated with the TGE process.

2.5 Standards describing general guidelines

2.5.1 SmartOne 5002

Title: Token Generation Event Standard – Code of practice controls

Scope: This Standard provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving a compliant TGE.

Purpose: provides guidance on the implementation of TGE controls.

2.6 Benefits of the SmartOne TGE family of Standards

The benefits of implementing a SmartOne TGE process will primarily result from a reduction in risk (i.e. reducing the probability of, and/or impact caused by, a TGE not meeting regulatory requirements). Specifically, benefits realised for an organization to achieve an TGE from the adoption of the family of standards include:

- A structured framework supporting the process of specifying and implementing a TGE that meets the organizations needs
- Assistance for management in creating the TGE in a responsible manner within the context of corporate risk management and governance
- Promotion of globally accepted good TGE practices in a non-prescriptive manner, giving organizations the latitude to adopt and improve controls that suit their specific circumstances
- Provision of a common language and conceptual basis for TGEs, making it easier to place confidence in business partners with a compliant TGE
- Increase stakeholder trust in the organization
- Satisfying societal needs and expectations
- More effective management of the TGE

2.7 Wording used in this Document

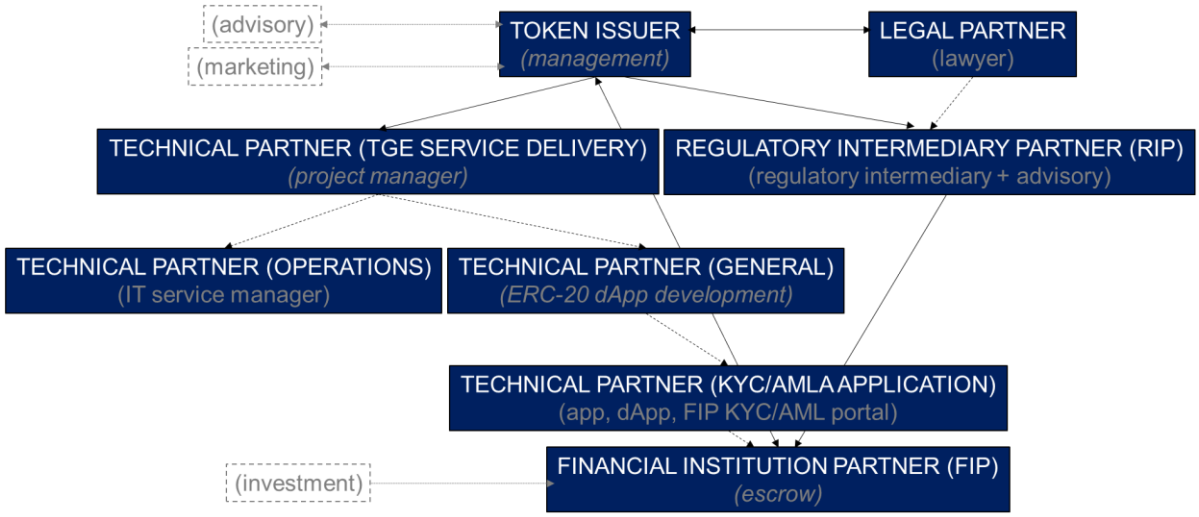
In all SmartOne Standards, the following words and meanings are used:

- 'shall' and 'shall not' indicate requirements to be strictly followed in order to conform to the document and from which no deviation is permitted
- 'should' and 'should not' indicates a recommendation which is particularly suited, but without excluding others, or that (in the negative form) a certain possibility is deprecated but not prohibited
- 'may' or 'may not' indicates a course of action which is permissible within the limits of the document
- 'can' or 'cannot' indicates a possibility or a capability

Information marked as 'Note' is for guidance in understanding or clarifying the associated requirement. 'Notes to entry' provide additional information that supplements the terminology and can contain provisions relating to a specific term.

2.8 Partners & Roles

The series of Standards makes references to Partners to facilitate some aspects of the TGE process. For example, a Technical Partner for application development or a Regulatory Institution Partner for an advisor to be the regulator intermediary. It should be noted however, that Partner does not specifically mean an external entity. The partners outlined are to be considered as more identified roles which must be filled. The Standard assumes an external entity to the Organization so that it is generic, but it may be that the Organization fills these roles with internal skills and that is permissible. A suggested mapping of partners and roles is illustrated below:



3 Terms and definitions

3.0.1

audit
systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

3.0.2

acceptance testing
formal testing of a system or application with respect to user needs, requirements and business processes. Conducted to determine whether or not a system satisfies the acceptance criteria.

3.0.3

Agreements
any agreement between two or more companies or organizations for the delivery of a service, resource or information.

3.0.4

algorithms
an unambiguous specification for a set of rules that precisely define a set of operations. In particular, this references cryptographic algorithms including key and block sizes.

3.0.5

anti-money laundering
The objective of anti-money laundering is to protect any financial system from money laundering and the financing of terrorism. Anyone who provides payment services or who issues or manages a means of payment is a financial intermediary who should be subject to AMLA regulations.

3.0.6

asset tokens
Asset tokens represent assets such as debt or equity claim on the issuer. Asset promise, for example, a share in the future organization earnings or future capital flows. These tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the blockchain may also fall into this category.

3.0.7

authentication
provision of assurance that a claimed characteristic of an entity is correct.

3.0.8

blockchain
a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retrospectively, without the alteration of subsequent records.

3.0.9

business model
a discussion on how the business operates, how it proposes to utilize and integrate with the blockchain and evidence of the need for the application or service.

3.0.10

category of token
identification of the type of token being issued by the Token Generation Event. Examples would include payment, utility or service.

3.0.11

certificated securities
securities which are in physical form.

3.0.12

change control procedure
a formal and documented procedure on how a business implements change.

3.0.13

content id hash
the generation of a fixed-size alphanumeric string by applying a cryptographic hash function to the content of the submission pack. The ID is a unique identifier for the submission pack, but the contents of the pack cannot be reverse engineered from the ID. This is also known as the hash value, message digest or digital fingerprint.

3.0.14

contributors
an investor who partakes in the Token Generation Event and receives tokens, of some classification, in exchange for fiat or cryptocurrency.

3.0.15
control
a measure that is modifying a risk.

3.0.16

crypto deposits
a store of cryptocurrency.

3.0.17

cryptocurrency
any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions.

3.0.18

cryptographic controls
the use of cryptography to protect the confidentiality, authenticity and integrity of information.

3.0.19

cryptographic keys
the string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. Keys will be symmetric or asymmetric. Symmetric encryption uses the same key to encrypt and decrypt. Asymmetric encryption uses 2 mathematically related keys, one for encryption and one for decryption.

3.0.20

cryptographic policy
the cryptographic requirements of the organization for the use of encryption techniques to protect sensitive data both at rest and in transit, as formally expressed by its executive management.

3.0.21

decentralized software architecture
a style of software architecture which has no infrastructural central point of failure.

3.0.22

de-registration
the act of removing an users account from a system or service.

3.0.23

development environment
an isolated infrastructure used solely for the development and testing of an application or a service. The infrastructure should mirror the production environment but contain no production data.

3.0.24

domicile
country or state of incorporation or registration of a firm where it has its legal address or registered office, or which is considered in law as the center of its corporate affairs.

3.0.25

dual-wallets
a hardware wallet that requires two parties to authenticate to obtain access.

3.0.26

economic model
a documented financial position of the business model. It will consider market size, cost base, quantity of tokens, entry and exit token positions, token burning and token economics.

3.0.27

escrow
an agreement between two people or organizations in which money or property is kept by a third person or organization until a particular condition is met.

3.0.28

executive management
person or group of people responsible for the implementation of strategies and policies to accomplish the purpose of the organization. Typically, this will be the top management and include roles such as Chief Executive Officer, Chief Financial Officer, Chief Technical Officer and Chief Information Officer.

3.0.29

fiat
legal tender whose value is backed by the government that issued it.

3.0.30

financial institution
an organization that conducts financial transactions.

3.0.31

forks
the blockchain is a distributed ledger made up of blocks of transactions that continuously grows, forming a single chain of blocks. Participants in the network must agree on a common set of rules to validate transactions in order to achieve consensus. A temporary fork occurs when there is a split in consensus and is part of the normal operation of the blockchain. However, a hard fork can also occur when there is a change in the underlying rules of the blockchain which is not backwards compatible and results in a permanent divergence of the blockchain.

3.0.32

Foundation
a not-for-profit organization the performs research into and promotes blockchain technology.

3.0.33

hard cap
the maximum number of tokens to be issued during a Token Generation Event.
3.0.34

hybrid tokens
Individual tokens that can be classified as both service and utility tokens.

3.0.35

identity verification
a method to ensure that users or customers provide information that is associated with the identity of a real person and that person is themselves. The process may be undertaken by the verification of authenticity of physical identity documents or information against authoritative sources.

3.0.36

information security
preservation of confidentiality, integrity and availability of information.

3.0.37

initial coin offering (ICO)
an ICO is where investors transfer funds, in the form of cryptocurrencies or fiat currencies to the ICO organizer. In return, they receive a quantity of blockchain-based coins which are created and stored in a decentralised form either on a blockchain specifically created for the ICO or through a smart contract on a pre-existing blockchain. Equally, there are several ways in which ICOs may be covered by existing financial market regulation.

3.0.38

intellectual property rights
the general term for the assignment of property rights through patents, copyrights and trademarks. These property rights allow the holder to exercise a monopoly on the use of the item for a specified period.

3.0.39

interested parties
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

3.0.40

investors
an investor who partakes in the Token Generation Event and receives tokens, of some classification, in exchange for fiat or cryptocurrency.

3.0.41

know your customer
the due diligence activities that financial institutions and other regulated companies must perform to ascertain relevant information from their clients for the purpose of doing business with them. The objective of KYC is to prevent banks from being used, intentionally or unintentionally, for money laundering or funding terrorism.

3.0.42

lack of consensus
a divergence in the agreement of the state of the blockchain by participants of the decentralized network.

3.0.43

legal opinion
a documented position on a topic or subject, proffered by a legal institution.

3.0.44

legal partner
a legal institution which has signed an Agreement with the Organization for the provision of legal services.

3.0.45

level of risk
magnitude of a risk expressed in terms of the combination of consequences and their likelihood.

3.0.46

likelihood
chance of something happening.

3.0.47

liveness detection
a test built into an application, for the assessment that a person is alive and forms part of identity verification.

3.0.48

mining attacks / blockchain attacks
any attempt to subjugate or harm the mining process of a blockchain. Attacks may take many forms, from deliberate acts against the protocol itself to unintentional acts which undermine the efficiency of the blockchain. Typically, this can range from 51% attack, social engineering to application vulnerabilities.

3.0.49

mrz passport / id scanner
an application that can digitally scan and understand the machine-readable zone (MRZ) or a passport or other identification document.

3.0.50

multi-factor authentication
an authentication process that involves at least two different forms of evidence. Typically, this is something you know (a password) and something you have (a security token or pin).

3.0.51

non-conformity
non-fulfilment of a requirement.

3.0.52

non-disclosure agreements
a contract by which one or more parties agree not to disclose confidential information that they have shared with each other as a necessary part of doing business together.

3.0.53

one-time password
a password (or pin) that is valid for only one login session or transaction, on a computer system or application. OTPs are not vulnerable to replay attacks.

3.0.54

operational environment
an isolated infrastructure used solely for the delivery of an application or a service. This is also known as the production environment. Strict change control and authentication/authorization procedures should be in place and adhered to.

3.0.55

operations model
how an application or service will meet: the requirements of KYC and/or AMLA legislation; secure fiat and crypto currency movements and all other security controls.

3.0.56

organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives. It includes sole-traders, company, corporation, firm, enterprise, authority, partnership, charity or institution or part thereof and may be public or private.

3.0.57
Organization
the organization which is undertaking the Token Generation Event.

3.0.58

payment tokens
payment tokens are synonymous with cryptocurrencies and are tokens intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Cryptocurrencies give rise to no claims on their issuer. The issuing of payment tokens constitutes the issuing of a means of payment and as such, should be subject to anti-money laundering regulations.

3.0.59

permanent storage
the writing of digital information to a medium that is considered permanent (for example, hard disks).

3.0.60

personally identifiable information
any data that can be used to identify a specific individual. In particular, this will include name, an identification number, location data, an online identifier to factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a person. Within Europe, special categories of data exist which must also be considered: any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health and data concerning a person's sex life or sexual orientation.

3.0.61

policy
intentions and direction of the organization as formally expressed by its executive management.

3.0.62

politically exposed persons
people who hold high public office. PEPs are required to undergo enhanced due diligence with regards to anti-money laundering.

3.0.63

pre-financing
TGEs that offer only the prospect that will receive tokens at some point in the future and the tokens or the underlying blockchain are not yet developed are known as pre-financed TGEs.

3.0.64

pre-sale
TGEs where investors receive tokens which entitle them to acquire other different tokens at a later date are known as pre-sale TGEs.

3.0.65

privacy policy
intentions and direction of how an organization handles any customer, client or employee information, as formally expressed by its executive management.

3.0.66

privileged access
accounts which bestow more than simple user rights on a system or application. Typically used for the management and operation of the application or system.

3.0.67

provision of evidence
a document or set of documents that can be used to demonstrate a specific task or provision has been met.

3.0.68

provisioning
the allocation of rights for users within or on an application or system.

3.0.69

registration
the creation of user accounts and for use within or on an application or system.

3.0.70

Regulator
a person or body that supervises a particular industry or business activity.

3.0.71

regulator intermediary
an organization which is licensed by the Regulator to enforce the Regulators rules and requirements.

3.0.72

regulatory requirements
all rules laid out by the Regulator, specific to each market sector.

3.0.73

requirement
need or expectation that is staged, generally implied or obligatory.

3.0.74

risk
effect of uncertainty on objectives.
3.0.75

risk acceptance
informed decision to take a particular risk.

3.0.76

risk analysis
process to comprehend the nature of risk and to determine the level of risk.

3.0.77

risk assessment
overall process of risk identification, risk analysis and risk evaluation.

3.0.78

risk evaluation
process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

3.0.79

risk management
coordinated activities to direct and control an organization with regard to risk.

3.0.80

residual risk
risk remaining after risk treatment

3.0.81

risk treatment
process to modify risk. Treatment may include a) avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; b) taking or increasing risk in order to pursue an opportunity; c) removing the risk source; d) changing the likelihood; e) changing the consequences; f) sharing the risk; g) retaining the risk by informed choice.

3.0.82

roadmap
a documented strategic direction of the organization, illustrating key milestones for the business, as defined by the executive management.

3.0.83

role based access control
a system of access control based around role assignment, role authorization and permission authorization.

3.0.84

secret information
any information pertaining to a user and their authentication process.

3.0.85

securities
securities in the sense of financial markets are standardised certificated or uncertificated proof of ownership or debt that has been assigned a value and may be sold. It represents an investment as an owner, creditor or rights to ownership upon which the holder hopes to gain profit.

3.0.86

self-regulatory organization
self-regulatory organizations (SROs) are regulatory intermediaries and as such, are subject to supervision by the Regulator. The SRO must be licensed and recognized by the Regulator.

3.0.87

smart contract
a smart contract, also known as a cryptocontract, is a computer program that directly controls the transfer of digital currencies or assets between parties under certain conditions.

3.0.88

Solidity
is the contract-orientated programming language for writing smart contracts.

3.0.89

Standards
document specifying authorized ways to achieve designated goal.

3.0.90

strong authentication
synonymous with multi-factor authentication. Typically, it requires at least two forms of authentication, but these may not be in the form of 'something you have' and 'something you know'.

3.0.91

submission content id hash
see content id hash

3.0.92

technical partner
an organization which has signed an Agreement with the Organizationfor the provision of technical services.

3.0.93

token classification
Each financial regulator will classify tokens in some way. Typically, this will be on the underlying economic function of the token. Individual token classifications are not mutually exclusive. Asset and utility tokens could also be classified as payment tokens and known as hybrid tokens.

3.0.94

token generation event
a TGE is where investors transfer funds, in the form of cryptocurrencies or fiat currencies to the TGE organizer. In return, they receive a quantity of blockchain-based tokens which are created and stored in a decentralised form either on a blockchain specifically created for the TGE or through a smart contract on a pre-existing blockchain. Unlike coins, the tokens are highly programmable and multifunctional.

3.0.95

token issuer
the organization generating tokens as part of a token generation event.

3.0.96

token seller
the investor selling tokens obtained at a token generation event or subsequent to that.

3.0.97

tokens
the digital asset to which value is attached. See payment tokens, utility tokens, asset token and securities.

3.0.98

uncertificated securities
securities which are in not in physical form.

3.0.99

utility tokens
utility tokens are tokens which are intended to provide access digitally to an application or service by means of a blockchain-based infrastructure.

Anti-money laundering regulations should not be applicable to utility tokens as long as the main reason for issuing tokens is to provide access rights to a non-financial application of blockchain technology.

3.0.100

wallet
a digital method for storing private keys. The wallet may be a hardware device or an application.

3.0.101

white paper
an authoritative report or guide, produced by the executive management of the Organization, to infirm potential investors about its proposal.