SmartOne STANDARD 5001

First Edition
2018-11

Token Generation Event Standard - Requirements

Contents

Foreword

SmartOne is established as a Foundation with the intention of serving both as a provider of legal services to Token Generating Event organisers 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.

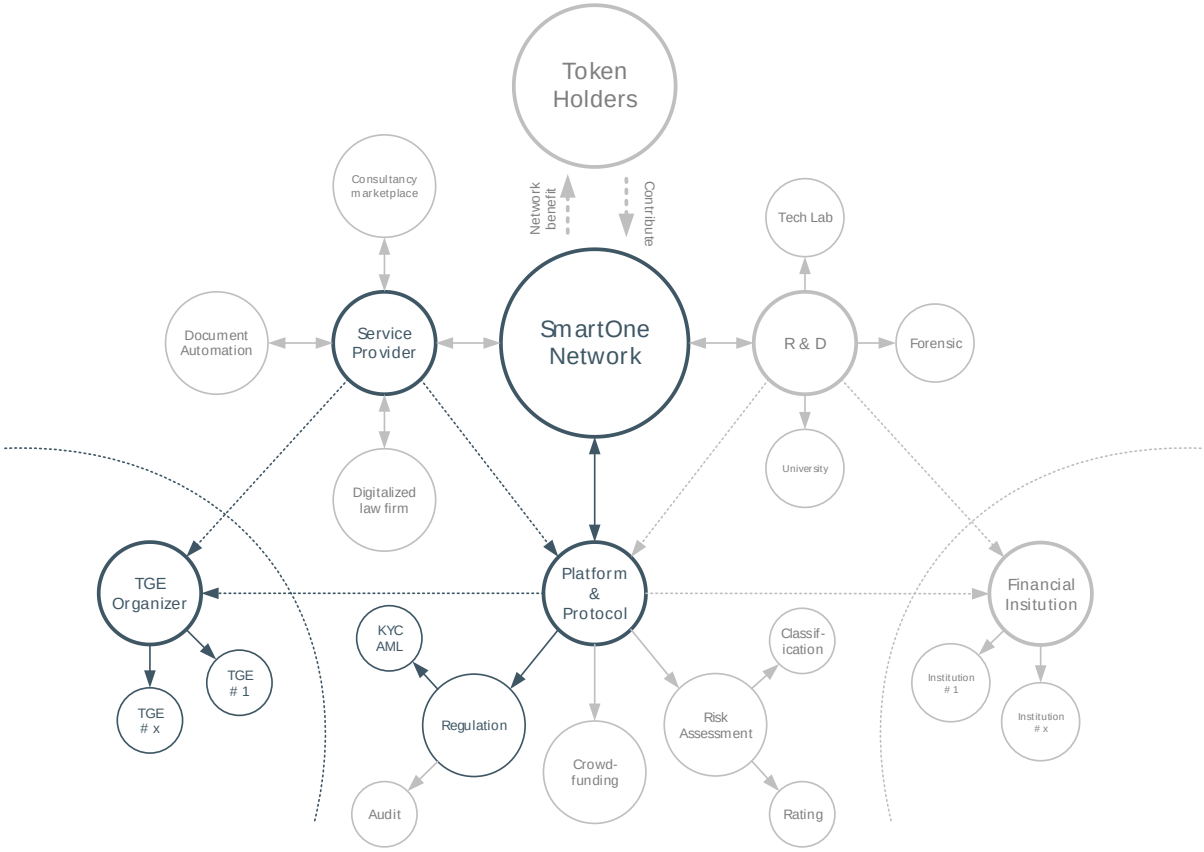
Attention is drawn to the possibility that some elements of this document may be subject of patent rights. SmartOne shall not be held responsible for identifying any or all such patent rights.

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

Introduction

0.1 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 ICO/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 ICO/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 ICO/TGE.

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

1 Scope of this Standard

This Standard specifies the requirements for establishing and implementing a compliant TGE/ICO. It also includes requirements for the assessment and treatment of risk tailored to the needs of the Organization. The requirements set out are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

2 Normative References

The following documents, in whole, or in part, are normatively referenced in this document and are indispensable for its application.

SmartOne 5000 – Overview and vocabulary

3 Terms and Definitions

For the purposes of this document, the terms and definitions given in SmartOne 5000 apply.

4 Initiating the TGE Process

4.1 Understanding the organizational context

By following the Standard, the Organization wishing to undertake a Token Generation Event can do so in a structured and efficient manner. The Standard also allows the Organization to meet regulatory demands on TGE's which have been sadly lacking in the formative months of ICOs/TGEs.

It is important that any organization understands the factors which will control and shape the success or failure of a TGE. This Standard will allow the Organization to develop a full understanding of the external and internal factors in play and help make the TGE process a success, both in operation but also as an on-going business proposition.

4.2 The importance of competence

The Organization must have the resources needed for the establishment and implementation of the TGE. This may come from external partners or internal employees. In either case, the people involved must have the required competence for their allocated role and/or responsibilities.

An evaluation must be undertaken to assure the Organization that all persons/partners are competent on the basis of appropriate education, training or experience.

Appropriate documentation should be retained as evidence of competence.

4.2 The needs and expectations of interested parties

For a regulatory complaint TGE, the organization must determine and understand 3 main items:

- Interested parties that are relevant to the TGE
- The requirements of these interested parties relevant to a TGE
- The requirements of any applicable Regulator and/or legislation

4.3 Determining the scope of the TGE

In relation to a business, the Organization must establish the scope of the TGE. This means it must understand:

- The external and internal issues affecting the TGE. Externally this will include Regulators, Financial Intermediaries, Financial Institutions, Legal Partners, Technical Partners, Contributors and end users. Internally, this will be affected by the structure of the Organization, its size and the scale of the TGE
- The full needs and expectations of interested parties

Section A.5 of Annex A will allow an organization to address these points.

4.4 The TGE policy

The Organization shall establish and maintain a TGE policy, in accordance with the requirements of this Standard. This will ensure that the policy covers:

- The TGE is appropriate to the purpose and direction of the Organization
- It includes TGE security objectives
- It includes a commitment to satisfy regulatory requirements

4.5 Control of documentation

Any auditable or certifiable process will necessitate the creation and maintenance of documentation to support it. Standard 5002, for example, discusses the mandatory and discretionary documentation needed for a TGE to meet the standard.

It is critical that this documentation be controlled, and the Organization should ensure that all documents:

- Use a standard and consistent identification template
- Are reviewed and approved by authorised people
- Are owned by a designated person or group of people
- Meet availability, confidentiality and integrity requirements of the Organization
- Are subject to change control process (i.e. version control)

5 Minimizing Risk

5.1 TGE risk assessment

Risk assessment is not covered by SmartOne Standards 5000, 5001 or 5002. There are many different risk models and risk-based approaches that the Organization may wish to use and SmartOne does not prefer one methodology over another. However, this step is an extremely critical step on the path to a successful TGE and must be undertaken.

A full and comprehensive risk assessment allows:

- A more likely success in the TGE achieving its desired outcome
- A reduction, if not prevention, of undesired or unseen effects

A SmartOne Standard will be available for undertaking a risk assessment but in the interim, the Organization must:

- Establish TGE risk criteria
- Identify TGE risks
- Analyse TGE risks

The Organization shall retain documented information about the TGE risk assessment process. The risk assessment will include:

- Leadership and commitment of the Organization to the TGE process
- Resource availability
- Partners and employee's competence
- Communications
- All technical, legislative and documentational controls as listed in Annex A

5.2 TGE risk treatment

The Organization shall define and apply an TGE risk treatment process to:

- Select appropriate TGE risk treatment options, taking into account the risk assessment results
- Determine all controls that are necessary to implement the TGE risk treatment options
- Compare the controls determined in this risk treatment process with those in Annex A of this document and verify that no necessary controls have been omitted.

- Produce a statement of applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not and the justification for exclusions of controls

The Organization shall retain documented information about the TGE risk treatment process.

6 Continuous evaluation

6.1 Management review

Management shall review the Organization's TGE planning and implementation at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

- The status of actions from previous management reviews
- Changes in external or internal issues that are relevant to the TGE
- Feedback on security performance
- Feedback from interested parties
- Results of risk assessment and status of risk treatment plans
- Opportunities for improvement

The Organization shall retain documented information as evidence of the results of management reviews.

ANNEX A

Reference objectives and controls

The control objectives and controls listed in the Table below are directly derived from and aligned with those listed in SmartONE 5002.

A.7 BUSINESS OBJECTIVES		
A.7.1 MANAGEMENT		
To ensure complete and comprehensive management oversight of the Token Generating Event		
A.7.1.1	Development of the TGE business model	CONTROL A set of documents for the business model of the TGE shall be defined, approved by management, published and communicated to employees and relevant external third parties.
A.7.1.2	Development of the TGE economic model	CONTROL A set of documents for the economics model of the TGE shall be defined, approved by management, published and communicated to employees and relevant external third parties. This shall be in alignment with the business model.
A.7.1.3	TGE partners	CONTROL Identification of TGE technology, legal, financial and regulatory partners.
A.7.1.4	Review of regulatory information	CONTROL The market specific, and/or region specific, regulatory requirements shall be reviewed to ensure continuing suitability, adequacy and effectiveness of the application or service to meet the requirements.
A.7.1.5	Review of Anti-Money Laundering Acts	CONTROL Requirements to meet AMLA shall be reviewed and documented.
A.7.1.6	Development of TGE operations model	CONTROL This shall cover the use of the Regulatory Intermediary to KYC/AMLA checks, escrow services, FIAT deposits, crypto deposits.
A.7.1.7	Collection of critical business information	CONTROL Collection of minimum information requirements to meet regulatory demands for the TGE.
A.7.1.8	Price and Payment procedure	CONTROL There shall be a formal and documented price and payment procedure for the TGE.

A.7.1.9	TGE security roles and responsibilities	CONTROL All TGE security responsibilities shall be defined and allocated.
A.7.1.10	Information Security Policy	CONTROL The Organization shall create and maintain an Information Security Policy for all aspects of the application or service and the project which delivers it.
A.7.1.11	Development of the TGE white paper	CONTROL The TGE white paper, shall be defined, approved by management, published and communicated to all relevant external third parties.

A.8 ENGAGEMENT WITH PARTNERS

A.8.1 GENERAL

General controls in relation to all business partners

A.8.1.1	Establish terms and conditions of all partnerships	CONTROL Legal, Technical, Regulatory Intermediary and Financial institutions must be selected and engaged with.
A.8.1.2	Screening	CONTROL Background verification checks on partners and/or suppliers.
A.8.1.3	Contact with authorities	CONTROL Contacts should be maintained by with regulatory bodies.
A.8.1.4	Monitoring and review of supplier services	CONTROL Organizations shall regularly monitor, review and audit supplier service delivery.
A.8.1.5	Confidentiality or non-disclosure agreements (NDA)	CONTROL Non-disclosure agreements shall be in place, if applicable.

A.8.2 LEGAL PARTNER

Controls in relation to the legal partner of the TGE

A.8.2.1	Identification of applicable legislation and contractual requirements	CONTROL All relevant legislative statutory, regulatory, contractual requirements shall be explicitly identified, documented and kept up to date for each system.
A.8.2.2	Token Sale terms	CONTROL An appropriate set of Token Sale Terms shall be ratified by the Legal Partner.
A.8.2.3	Legal opinion	CONTROL

		The Legal Partner shall give its opinion on the TGE as to the category of the tokens.
A.8.2.4	Engagement with Regulators	CONTROL The relevant regulators shall be informed of the legal opinion and proof obtained of the adherence to the regulatory framework for that Token type.
A.8.2.5	Privacy Policy	CONTROL The Organization shall develop and maintain a privacy policy for all external 3rd parties, including partners and token holders.
A.8.2.6	Identification of token delivery parties	CONTROL The Legal Partner shall identify all parties required for token delivery. These may include trustee's and/or transfer agents.

A.8.3 TECHNICAL PARTNER (GENERAL)

General controls in relation to the Technical Partner of the TGE. Applicable to all technical solutions delivered by the partner.

A.8.3.1	Identification of required blockchain contracts	CONTROL Documented review of required contracts for all regions the TGE is applicable.
A.8.3.2	Development of Smart Contracts	CONTROL Development and publication of smart contracts on the blockchain for tokens and token delivery. This may include trustee and/or transfer agents.
A.8.3.3	Blockchain integration	CONTROL The Technical Partner should deliver a solution that is fully integrated with blockchain technology.
A.8.3.4	Outsourced development or delivery	CONTROL The Organization shall develop and maintain a policy for outsourcing technical delivery of TGE components. The Organization shall supervise and monitor the activity of any system delivered by an outsourced software component.
A.8.3.5	Separation of development, testing and operational environments	CONTROL Where the Technical Partner operates a service or application on behalf of the Organization, it must operate separate development, testing and operational environments.
A.8.3.6	System security testing	CONTROL The Organization shall develop and maintain its own acceptance testing policy. The Organization may outsource security testing to utilise technical expertise of a Partner, but it remains responsible for its delivery.
A.8.3.7	System acceptance testing	CONTROL

		The Organization shall develop and maintain its own acceptance testing program.
A.8.3.8	Secure development policy	CONTROL The Organization shall enforce a secure development policy of its Technical Partner.
A.8.3.9	Secure development environment	CONTROL The Organization shall enforce a secure development environment of its Technical Partner.
A.8.3.10	Securing application services	CONTROL Information involved in the application must be protected against fraudulent activity, unauthorized disclosure and modification.
A.8.3.11	Information security requirements analysis and specification	CONTROL Information involved in the application must be protected against fraudulent activity, unauthorized disclosure and modification.
A.8.3.12	Policy on the use of cryptographic controls	CONTROL A policy on the use of cryptographic controls for the protection of information should be developed and implemented.

A.8.4 TECHNICAL PARTNER (KYC/AMLA APPLICATION)

Controls in relation to the delivery of the KYC application by the Technical Partner of the TGE.

A.8.4.1	KYC Functionality	CONTROL The Technical Partner shall deliver a full KYC application to meet the appropriate regulatory requirements.
A.8.4.2	Information transfer policies and procedures	CONTROL Formal transfer policies, procedures and controls should be in place to protect the transfer of information.
A.8.4.3	Protecting application services transactions	CONTROL Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
A.8.4.4	KYC+AML apps and portal operations	CONTROL The KYC application shall have a defined and secure process to download and approve/reject the KYC pack submission.
A.8.4.5	Integration with blockchain	CONTROL The KYC process shall be fully integrated with the blockchain technology including app submission, approval and token issuance.
A.8.4.6	Notification process	CONTROL

		Participants shall be informed of KYC progress through a defined set of methods.
A.8.4.7	Privacy and protection of personally identifiable information	CONTROL Privacy and protection of personally identifiable information shall be ensured.
A.8.4.8	Secure log-on procedures	CONTROL Employee access to the KYC packs shall be secured through multi-factor authentication.

A.8.5 TECHNICAL PARTNER (TGE SERVICE DELIVERY)

Controls in relation to the delivery of the Token Generation Event by the Technical Partner.

A.8.5.1	Secure system engineering principles	CONTROL The Organization must set out the engineering principles it requires of its Technical Partner or assess its Technical Partners own principles to ensure that they are in alignment.
A.8.5.2	System change control procedures	CONTROL Changes to systems within the development lifecycle shall be controlled using formal change control procedures. Formal change control procedures should be developed and maintained.
A.8.5.3	Technical review of applications after changes	CONTROL After any change, the application must be reviewed for functionality.
A.8.5.4	Key management	CONTROL A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented.

A.8.6 TECHNICAL PARTNER (OPERATIONS)

Controls in relation to the operation of any application delivered by the Technical Partner of the TGE.

A.8.6.1	Segregation of duties	CONTROL Conflicting duties and areas of responsibility shall be segregated.
A.8.6.2	Access control policy	CONTROL An access control policy shall be established, documented and reviewed based on business requirements.
A.8.6.3	Management of secret information of users	CONTROL A process should be developed and maintained to protect secret information.
A.8.6.4		CONTROL

	User registration and de-registration	A formal user registration and de-registration process should be implemented to enable the assignment of access rights.
A.8.6.5	User access provisioning	CONTROL Any application shall have defined role-based access control to participants information – access control policy.
A.8.6.6	Management of privileged access rights	CONTROL The allocation and use of privileged access rights should be restricted and controlled.
A.8.6.7	Review of user access rights	CONTROL All access and use rights should be periodically reviewed.
A.8.6.8	Use of secret authentication information	CONTROL Implementing the information security policy with regards to the use of secret authentication information.
A.8.6.9	Information access control	CONTROL Role based access control shall be used.
A.8.6.10	Documented operating procedures	CONTROL Operating procedures should be documented and made available to all users who need them.
A.8.7 REGULATORY INTERMEDIARY PARTNER (RIP)		
Controls in relation to the Regulatory Intermediary Partner (or Self Regulatory Organization) of the TGE.		
A.8.7.1	Regulatory Intermediary status	CONTROL The RIP shall hold the relevant intermediary requirements/licenses of regulators and shall be subject to regulatory audits as needed to maintain their status.
A.8.7.2	Adoption of a KYC procedure	CONTROL The RIP shall adopt a KYC procedure for all TGE contributors.
A.8.7.3	Information transfer of the KYC	CONTROL Secure transfer of information between the organizations and external parties must be enforced.
A.8.7.4	Contact with the Regulator	CONTROL Collection of minimum information requirements to meet regulatory demands for the TGE.
A.8.8 FINANCIAL INSTITUTION PARTNER (FIP)		
Controls in relation to the Financial Institution Partner of the TGE.		
A.8.8.1	Financial Institution status	CONTROL The FIP shall provide services approved by the Regulatory Intermediary Partner.

A.8.8.2	Escrow accounts	CONTROL Provision of an escrow account, if applicable.
A.8.8.3	Escrow process	CONTROL Procedures for escrow account access shall be developed, if applicable.
A.8.8.4	Financial accounts	CONTROL Provision of all bank accounts, if applicable.
A.8.8.5	Process for fund transfer notification and token release	CONTROL If applicable, the FIP shall develop a process for the notification of all parties relevant to a fund transfer and token release. This may be in the form of a programmatic API call, electronic message or other means.

A.9 REGULATIONS

A.9.1 REGULATORY COMPLIANCE

General controls to meet regulatory requirements

A.9.1.1	Token Categorization	CONTROL An assessment must be made of the token type. The assessment must be agreed between the Organization and its Legal Partner.
A.9.1.2	Utility Tokens	CONTROL Assessment of the token as a utility token, where applicable.
A.9.1.3	Status of Tokens as Securities	CONTROL Assessment of the token as a security, where applicable.
A.9.1.4	Review of AMLA regulations	CONTROL Documented assessment of the latest AMLA regulations and their applicability to the TGE.
A.9.1.5	Application of the Anti-Money Laundering Act	CONTROL Documented evidence that the KYC process in place has been approved by the relevant Regulator.

A.10 RISK ASSESSMENT

A.10.1 BLOCKCHAIN

Risk assessment of all blockchain-related issues

A.10.1.1	Review of blockchain risks	CONTROL A risk assessment for all blockchain-related issues.

A.10.2 REGULATORY

Risk assessment of all regulatory-related issues

A.10.2.1	Review of regulatory risks	CONTROL A risk assessment for regulatory-related issues.