ITA Blueprint Guidelines

MDIA
Malta Digital Innovation Authority

ITA Blueprint Guidelines

Digital Innovation is, by definition, a rapidly evolving sector. These guidelines are expected to be updated to keep abreast with technology, regulatory and operational developments.

Document Version: 23 August 2019 version change 2

Contents

1. Definitions

"Applicant", within the context of this document, refers to an individual and/or legal organisation applying for Certification of an Innovative Technology Arrangement (ITA) with the Authority.

"Authority" refers to the Malta Digital Innovation Authority ('MDIA').

"Blueprint" refers to a document that includes a description of the qualities, attributes, features, behaviours or aspects of an ITA as defined by the respective Lead Authority.

"Distributed Ledger Technology", 'DLT', 'distributed ledger technology', 'decentralised ledger technology' means a database system in which information is recorded, consensually shared, and synchronised across a network of multiple nodes, or any variations thereof, as further described in the First Schedule of the Innovative Technology Arrangements and Services Act, 2018 ('ITAS'), and the term "node" means a device and data point on a computer network;

"Innovative Technology Arrangement", also referred to as 'ITA' within this document, as defined within the First Schedule of the Innovative Technology Arrangements and Services Act, 2018. It means the intrinsic elements including software, codes, computer protocols and other architectures which are used in the context of DLT, smart contracts and related applications as well as other arrangements as may be further defined in the Innovative Technology Arrangements and Services Act, 2018. For the avoidance of doubt, this definition includes, inter alia, any ITA supporting an IVFAO, Providers of VFA Services or similar arrangements.

"Lead Authority" refers to the 'national competent authority' as defined within the Innovative Technology Arrangements and Services Act, 2018, which has a leading role within that application of the ITA.

"Smart Contract", as defined within the Virtual Financial Assets Act, 2018, means a form of innovative technology arrangement consisting of:

a) a computer protocol; and, or
b) an agreement concluded wholly or partly in an electronic form, which is automatable and enforceable by execution of computer code, although some parts may require human input and control and which may be also enforceable by ordinary legal methods or by a mixture of both.

"Systems Auditor" ('SA') as defined in the Innovative Technology Arrangements and Services Act, 2018, and in line with further guidance issued by the Authority within the 'Systems Auditor Guidelines'.

2. Blueprint of the ITA

2.1. Scope

The Blueprint is a document which highlights all of the critical and important features which an ITA should include in the information submitted to the Authority during the application for the ITA certification. This document will also be used by the Systems Auditor to understand and verify the implementation of the control objectives as described in 'Chapter 1 – Systems Auditor Guidelines'.

The Blueprint is split into the following requirements, as documented in 'Chapter 2 – Innovative Technology Arrangements Guidelines':

- Purposes: The reasons for which the ITA is being, or was, created
- Qualities: The specific characteristics that the ITA offers to its users
- Aspects: The specific elements or boundaries of the ITA that are subject to the certification
- Features: The distinctive functional capabilities of the ITA
- Attributes: The inherent capabilities of the ITA
- Behaviours: The manner how the ITA responds to unexpected processes and inputs
- Limitations: The technical and/or operational restrictions of the ITA

The next sub-sections explain the level of detail that would typically be expected in the Blueprint documentation of the ITA.

2.2. High-level description

The Applicant needs to provide a high-level description regarding the scope and purpose that the ITA fulfils. As a minimum, such a description should include:

- What user demands is the ITA addressing
- What benefits the user will derive from when making use of such an ITA
- What expected benefits will the Applicant derive from the ITA
- To what type of audience is the ITA designed to address
- How was quality assurance practised during the development and/or implementation of the ITA

2.3. Technical qualities

The Applicant needs to provide a detailed description of the ITA that is being submitted for registration with the Authority. The information provided needs to be in-line with the Technology Stack described in the 'Technology Stack Nomenclature'. The Authority is providing further guidance below on what information should be provided for each

of the layers within the technology stack, in the form of a questionnaire to be answered by the applicant of the ITA. The questions should not be considered exhaustive.

For each of the layers described below, explain:

- How fidelity to the claimed functionality is being addressed
- How is privacy, integrity and confidentiality is being addressed
- Describe what programming language was used and/or technologies which the ITA is dependent on
- Are any access control mechanisms in place
- Describe what external interface the ITA offers
- Describe any external dependency the ITA requires
- Describe the DLT metrics that are relevant to the functionality of the ITA
- What underlying technologies is the ITA specifically making use of - the Applicant is requested to provide a high-level diagram of the ITA
- How the ITA handles data - the ITA should provide a high-level data flow diagram showing how data flows between the various components of the ITA

Off-DLT Application Layer

- Does the ITA use any third party platforms, such as other ITAs? If that is the case, provide description of how this is implemented.
- Is there any processing done outside of the ITA?
- Are there any dependencies or links to other data sources?

DLT Application Layer

- Describe the features and functions within the application layer, including any capabilities which tackle any regulatory obligation.
- Describe the logic behind the DLT application.
- Does the ITA have any performance requirements?
- How is data protection by design and/or data protection by default implemented?
- Describe any automated and/or manual error correcting mechanisms in place
- Are there any immutable/mutable characteristics within the ITA? If that is the case, provide a description and explain how these characteristics are implemented.

DLT Implementation Layer

- Describe the features and functions within the implementation layer, including any capabilities which tackle any regulatory obligation.
- Are any specific mining resources or other dependencies required to reach consensus?
- How is scalability addressed?
- Are there inherent limitations on scale?

- How is the creation of new nodes/blocks addressed?
- Describe the consensus process of the ITA.
- Are there any availability safeguards built into the ITA?
- How is integrity of the data within the ITA secured?
- Describe any secure communication protocols in use.
- Does the ITA split its functionality between public and private blockchain setups?

Networking, Infrastructure and Physical Layer

- How can the network be accessed?
- Identify any particular infrastructure requirements.
- Describe the hardware or virtual factors required in order for the ITA to function correctly.
- Describe any availability safeguards built into the ITA from a physical perspective

2.4. Forensic Node

For details on the Forensic Node, please refer to separate MDIA guidelines dedicated to this topic. The Forensic Node guidelines are available on www.mdia.gov.mt in *Guidelines* section of the website. The Forensic Node guidelines are available on www.mdia.gov.mt in "*Guidelines*" section of the website.

2.5. Information security requirements

A risk assessment should be undertaken and documented on the ITA. Such a risk assessment may include the following information:

- Risk reference
- Risk description
- Risk type
- Scenario
- Threat actor
- Affected assets
- Risk owner
- Original risk rating
- Implemented mitigation controls
- Effectiveness of control
- Likelihood of happening
- Inherent risk
- Residual risk
- Financial impact value of risk

The Authority requires all Applicants to provide information based on the following:

- Describe how a security risk assessment plan was undertaken and is maintained.
- How is information security being addressed?
- Provide information on what information security algorithms are being deployed and implemented.

2.6. TA powers of intervention

In line with Article 8(4)(d)(iii) of the ITAS Act, the ITA needs to document within the Blueprint the powers and the technology features proposed to enable the Technical Administrator, or the Authority (in the case of unjustifiable failure by the Technology Administrator) to intervene in the event of:

- A material cause of loss to any user
- A material breach of law

Such intervention would need to be conducted in a transparent and effective manner. It must address the cause of loss or the breach of law such that it does not occur or re-occur.

The Authority requires the Applicant to:

- Provide information on the possibility for someone to intervene during the ITA's activity. If there is no power to intervene, the Applicant needs to explain in detail the reason why intervention on the ITA's activity is not technically feasible.
- Provide the documented procedure required to intervene upon the ITA.
- Provide details of the authorised persons or entities who can intervene upon an ITA.

2.7. Other information

The Authority requires other information that is not of a technical nature.

- Provide information on the governance structure of the ITA.
- Describe any limitations or restrictions on the operational boundaries of the system.
- Describe any specific features that distinguish the ITA from other ITA projects of a similar nature.
- Is there any expected end-of-life date or event for the ITA?
- Are there any risks that may cause the ITA to reach its end-of-life prematurely?
- Document how forking circumstances can occur and how they would be addressed.

3. Conclusion

The Authority is issuing, as a separate document, the 'Technology Stack Nomenclature' that describes further it's understanding of the Technology Stack outlined above.