

Chapter 02

# Innovative Technology Arrangement Guidelines

---



## MDIA Circular No.2

As already communicated, the MDIA will be issuing a set of guidance notes aimed at assisting Service Providers and Innovative Technology Arrangements seeking recognition by the MDIA. These guidelines will be divided into four chapters as follows:

- Chapter 1 Systems Auditors Guidelines (*consultation period ends 02 October 2018*)
- Chapter 2 Innovative Technology Arrangement Guidelines
- Chapter 3 Technical Administrator Guidelines
- Chapter 4 Resident Agent Guidelines

The MDIA is pleased to announce the second round of consultation (Ref No.02/18) which is covering three areas, namely:

1. Proposed changes to the Innovative Technology Arrangements and Services Act ('ITAS Act');
2. Chapter 2 of the MDIA Guidance Notes; and
3. Proposed fee structure.

### Concluding remarks

The consultation period is open to the public from 26 September 2018 until 09 October 2018. Interested parties are requested to submit their comments and feedback by email on [info@mdia.gov.mt](mailto:info@mdia.gov.mt) by not later than 09 October 2018.

**Malta Digital Innovation Authority**  
**26 September 2018**

## 1. Proposed changes to the ITAS Act

Following feedback received by the Authority and discussions taking place, the MDIA shall be making proposals to amend the Innovative Technology Arrangements and Services Act, 2018<sup>1</sup> ('ITAS Act'). The proposed amendments concern the following:

### a. Role of the Technical Administrator and Certification issued by the MDIA

It is acknowledged that, in specific ITA implementations, the functionality to grant the Technical Administrator and the Authority, where applicable, power to intervene, as required in Article 8(4)(c)(iv) and Article 8(4)(d)(iii) of the ITAS Act, may not be technically feasible or justifiable. In this regard, when it is clearly justified as to why the implementation of such functionality cannot be achieved, the Authority reserves the right to vary this requirement. In doing so, subject to all other requirements being successfully met by the Applicant, the Authority may issue an ITA certification that clearly states that the requirements of Article 8(4)(c)(iv) and Article 8(4)(d)(iii) of the ITAS Act are not being achieved. In addition, the Applicant shall be required to disclose such limitation to all users as part of the Terms of Service.

### b. Material changes

Article 12 of the ITAS Act indicates the instances when any person recognised by the MDIA needs to notify the MDIA with respect to material changes.

Proposals are being made so that recognised persons would need the MDIA's prior approval as opposed to a mere notification in certain instances. Details on these changes are reflected in Section 10 of Chapter 2 of the MDIA Guidance Notes which is being made available for consultation.

---

<sup>1</sup> Chapter 592 of the Laws of Malta

## **2. Chapter 2 – Innovative Technology Arrangement Guidelines**

The MDIA is making available for public consultation Chapter 2 – Innovative Technology Arrangement Guidelines.

This Chapter has been drafted taking into consideration the proposed changes (indicated under 1 above) to the ITAS Act as detailed above.

Chapter 2 – Innovative Technology Arrangement Guidelines shall apply to all interested applicants who shall seek a voluntary certification of their innovative technology arrangement, as defined in the Innovative Technology Arrangements and Services Act, 2018<sup>2</sup> as contemplated in the said Act.

The document is aimed to provide guidance to prospective applicants on:

- the application process;
- the process for certification of an innovative technology arrangement;
- documentation required for completeness of an ITA Certification Application;
- the general and specific requirements that an ITA is expected to meet; and
- on-going obligations of an ITA once MDIA certifies the arrangement.

## **3. Proposed fee structure**

The Authority is issuing the proposed fee structure in relation to the certification of Innovative Technology Arrangements (ITAs), registration of Systems Auditors and Technical Administrators, and other fees, for public consultation.

The MDIA is considering the possibility of incentivising start-ups through rebates and/ or other schemes. Feedback is being solicited on this matter.

---

<sup>2</sup> Chapter 592 of the Laws of Malta

## Certification Fees

Amounts in €		
<b>Certification of ITAs:</b>		
Processing fee:		
Stage 1: initial processing fee – payable concurrently with submission of application		2,000
Stage 2: the systems audit leading to ITA certification – payable concurrently with submission of Systems Audit report		3,000
Certification fee:  Valid for two years, after which certified ITAs need to re-apply to renew their certification for a further period of two years.  A fee of €40,000 is payable upon renewal.		40,000

## Registration fees

Amounts in €	Initial processing fee	Registration fee *
<b>Registration of:</b>		
Systems Auditors having up to 5 Subject Matter Experts **	7,500	15,000
Technical Administrators	5,000	10,000

\* Valid for two years, after which Systems Auditors and Technical Administrators need to re-apply to renew their registration for a further period of two years.

\*\* The initial processing fee for the registration of a Systems Auditor is increased by €500 for every additional Subject Matter Expert in excess of five Subject Matter Experts.

## Other fees

<b>Amounts in €</b>		
<b>Submission of Systems Audit report</b>		
Processing fee		3,000
<b>Appointment of Resident Agents</b>		
One-time processing fee		250
<b>Fees in relation to material changes in:</b>		
Software		1,000
Rights of users		500
Rights, authorisation or powers of Technical Administrator or the Authority		500
Technical Administrator		500
Administrator of a relevant legal organisation		1,500
Qualifying shareholders		1,500
Subject Matter Experts		500
Person with reference to whom a certification or Certificate of Registration has been issued:		
<ul style="list-style-type: none"> <li>Person has already been assessed by the MDIA</li> </ul>		500
<ul style="list-style-type: none"> <li>Person has not yet been assessed by the MDIA</li> </ul>		1,500
<b>Fines and penalties (up to):</b>		
Failure to seek MDIA prior approval for material changes		10,000
Failure to notify material changes to MDIA		7,500
Failure to inform MDIA of material changes within stipulated timeframes		2,500

## Chapter 2 - Innovative Technology Arrangement 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.

# Contents

Contents .....	2
1. Definitions .....	3
2. Applicability and Scope.....	4
3. Eligibility.....	5
4. Application Process.....	6
4.1. Stage 1.....	7
4.2. Stage 2.....	8
4.3. ITA Processing Fees.....	9
4.4. Documentation Required .....	10
5. General Requirements .....	12
6. Specific Requirements .....	13
6.1. Fit and properness .....	13
6.2. Positive assurance from Systems Auditor/s .....	16
6.3. Appointment of Technical Administrator/s.....	17
6.4. Compliance with applicable and mandatory law .....	19
6.5 Adequate disclosures to users .....	19
7. Resident Agent.....	20
8. Outsourcing .....	21
9. Certification.....	22
9.1. Full certification.....	22
9.2. Conditional certification .....	22
10. Ongoing obligations.....	24
10.1. Display of certificate.....	24
10.2. Go Live Date .....	24
10.3. Material Changes.....	24
10.4. Prior approval of the Authority.....	25
10.5. Notification to the Authority .....	25
11. Renewal process.....	27
Appendix I - Who is the Administrator?.....	28
Appendix II - Who are the Qualifying Shareholders?.....	30
Appendix III – Technology Stack and Use Cases .....	32

## 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’) as defined in the Malta Digital Innovation Authority Act.

“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. 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.

“Register of Recognitions” is an electronic register, also referred to as “the Register”, of all recognitions issued by the Authority, which recognitions shall include the certification of ITAs, and registration of Systems Auditors and Technical Administrators. The Register shall include all such details as the Authority shall consider necessary to identify the relevant Applicant and the activities being carried out. In addition, the Register shall be available to the public on the website of the Authority.

“Resident Agent” refers to the Resident Agent as defined in Article 15 of the Innovative Technology Arrangements and Services Act, and in line with further guidance issued by the Authority under Chapter 4 of the Guidance Notes.

“Systems Auditor” (‘SA’) as defined in the Innovative Technology Arrangements and Services Act, 2018, and in line with further guidance issued by the Authority under Chapter 1 of the Guidance Notes.

“Technical Administrator” (‘TA’) as defined in the Innovative Technology Arrangements and Services Act, 2018, and in line with further guidance issued by the Authority under Chapter 3 of the Guidance Notes.

## 2. Applicability and Scope

These Guidelines shall apply to Innovative Technology Arrangements ('ITAs') in terms of the Innovative Technology Arrangements and Services Act ('ITAS Act') seeking a voluntary certification by the MDIA.

In line with the Second Schedule of the ITAS Act, for the time being the following are to be considered as ITAs:

- a) software and architectures which are used in designing and delivering DLT which ordinarily, but not necessarily:
  - uses a distributed, decentralised, shared and, or replicated ledger;
  - may be public or private or hybrids thereof;
  - is permissioned or permission less or hybrids thereof;
  - is secure to a high level against retrospective tampering, such that the history of transactions cannot be replaced;
  - is protected with cryptography; and
  - is auditable.
  
- b) smart contracts and related applications, including decentralised autonomous organisations, as well as other similar arrangements.

The Minister for the Digital Economy, on the recommendation of the Authority, may designate any other innovative technology arrangement to fall in scope of these guidelines and relative guidance will be issued accordingly.

These guidelines outline the high-level standards that an ITA seeking voluntary certification from the Authority needs to follow.

The voluntary certification granted by the Authority covers a set of core features that the Authority deems essential to ensure that reasonable standards are met with respect to purpose, qualities, features, attributes, behaviours or aspects of the ITA.

### 3. Eligibility

Prospective ITAs may submit an 'Innovative Technology Arrangement Application Form' (ITA Application Form) to the Authority for certification of the technology arrangement.

For an application to be considered by the MDIA, the Applicant will need to include a justification why the certification is being sought clearly indicating:

- a) the mandate that entitles the Applicant to submit such an application; and
- b) the governance structure of the ITA.

In line with Article 8 of the ITAS Act, the MDIA will only certify ITAs once it is satisfied that the general and specific requirements of said article have been satisfied.

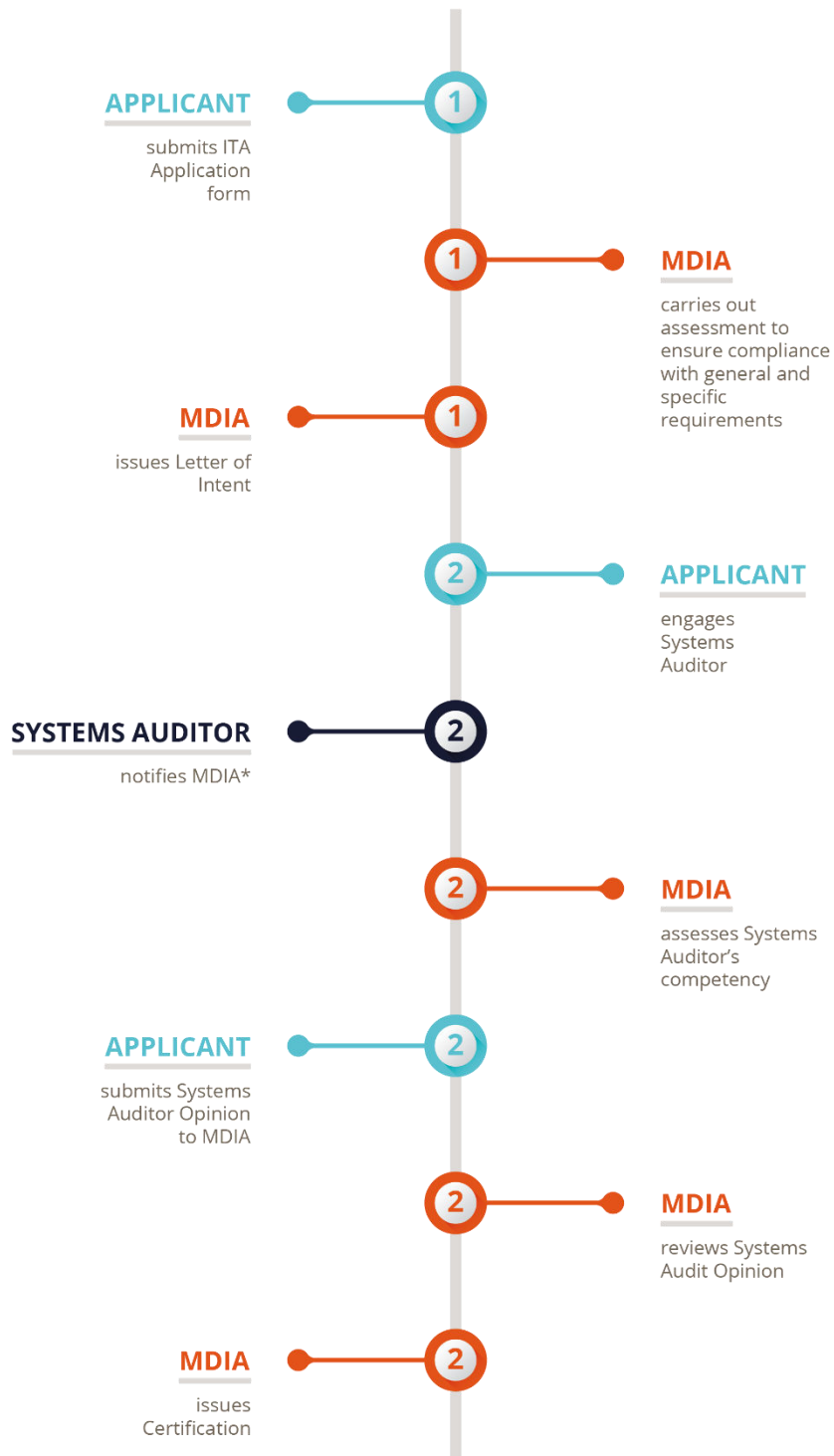
To determine this, the Authority will:

- Review and assess the information provided in the ITA Application Form;
- Review the documentation submitted as detailed in these guidelines, as well as, any additional documentation that the Authority may request;
- Carry out the necessary due diligence on the Applicant, including the Administrator and Qualifying Shareholders, as applicable;
- Assess whether the appointed Technical Administrator can fulfil such a role with respect to the ITA seeking certification; and
- Rely on the Systems Auditor opinion to confirm that reasonable standards with reference to the specific purposes, qualities, features, attributes, behaviours and/or aspects of the ITA are met. For details on the Systems Auditor and the Systems Auditor Report, refer to Chapter 1 of the MDIA Guidance Notes.

The Authority reserves the right to vary any of the requirements in particular cases upon reasonable justification. The Authority will ensure that this is done in a consistent and equitable manner.

## 4. Application Process

The application process for certification of an ITA is divided into two stages:



1: Stage 1    2: Stage 2

\*Refer to Chapter 1 of the MDIA Guidance Notes

During Stage 1 the Authority will assess the ITA's capability to meet the generic and specific requirements as stated in Articles 8(3) and 8(4) of the ITAS Act respectively, including the fit and properness of the Applicant, Administrator and Qualifying Shareholders. A satisfactory conclusion of Stage 1 will enable the Authority to issue a Letter of Intent to the Applicant. The Authority may indicate issues in the Letter of Intent that will impinge on the Authority's decision to grant certification to the Applicant if these are not addressed during Stage 2 of the Certification application process.

Upon receipt of the Letter of Intent, the Applicant must engage a Systems Auditor to carry out the Systems Audit as indicated by the MDIA in the Letter of Intent. Upon conclusion of the Systems Audit, the Applicant shall remit the Systems Auditor Report to the MDIA. The Authority will review the opinion provided by the Systems Auditor, assess if issues raised in the Letter of Intent have been satisfactorily resolved and if it deems that the ITA satisfactorily meets the criteria of the ITAS Act, proceed to grant the Certification.

In order not to delay the application process unnecessarily, the Authority recommends that the Applicant identifies a potential Systems Auditor prior to submitting the ITA Application Form. To assist in this identification process, the Authority draws to the attention of the Applicant the Register of Recognitions, which is available to the public and maintained by the Authority. The Register of Recognitions, contains amongst other listings, a list of Systems Auditors that have been granted recognition by the Authority to carry out Systems Audits. It is pertinent to note that a registered Systems Auditor must have suitable experience in the ITA to be audited. Therefore, the Authority strongly recommends prospective Applicants to identify a suitable Systems Auditor prior to submitting the ITA Application Form.

In appointing a Systems Auditor, the Applicant, together with the Systems Auditor would also need to take into consideration conflicts of interest. Further guidance on this matter can be found in Chapter 1, Part A, Section 6 of the MDIA Guidance Notes.

#### 4.1. Stage 1

The Authority will need to ascertain that the ITA meets the generic and specific requirements contemplated within the ITAS Act. Apart from looking at the technological aspect, prior to issuing a Certificate, the Authority will also need to ascertain that the Applicant of the ITA, as well as, key functionaries are of good repute and standing. In this respect, the Applicant is required to complete and submit an ITA Application Form to the Authority.

The ITA Application Form must be accompanied by:

- all the supporting documentation (*refer to Section 4.6 for details*);
- completed and signed Fit and Proper Questionnaires for the individuals indicated (*refer to Section 4.5 for details*); and
- the first non-refundable instalment of the Processing Fee (*refer to Section 4.3 for details*).

These three elements determine the completeness of an application.

The Authority will only process fully completed applications. In case of incomplete application forms, the Authority will indicate pending requirements to the Applicant. Processing of application shall not commence prior to receipt of outstanding items. If pending items remain outstanding after one (1) month from communication issued by the Authority without an explanation from the Applicant, the Authority will terminate the application process and shall inform the Applicant accordingly.

Upon receipt of a completed application, the Authority will commence its review process to ensure that:

- in principle, the ITA meets the generic and specific requirements; and
- the individuals / functionaries involved are fit and proper.

Once the Authority is satisfied that the above requirements are met, the Authority will provide the Applicant with a Letter of Intent and instruct the Applicant to formalise the appointment of the Systems Auditor and initiate the Systems Audit.

## 4.2. Stage 2

Following receipt of the Letter of Intent, the Applicant shall engage with the Systems Auditor to carry out the Systems Audit as indicated by the Authority. Upon conclusion of the Systems Audit and receipt of the Systems Auditor Report, the Applicant shall forward the Systems Audit Report to the Authority to initiate the second stage of the certification application process. This submission shall be accompanied by the second instalment of the Processing Fee.

Upon receipt, the Authority shall review the Systems Audit Report to establish whether following the opinion issued by the Systems Auditor, the ITA is adequately meeting the generic and specific requirements contemplated in the ITAS Act, as well as, the standards the Authority deems necessary for the certification sought. The Authority will also look at any elements highlighted in

the Letter of Intent, as well as, changes that occurred since the issuance of the Letter of Intent that could impact the ITA.

Upon a positive conclusion of this stage, the Authority will issue the Certification of the ITA and update the Register of Recognitions accordingly. In line with the Third Schedule of the ITAS Act, the ITA Certification shall be valid for a term of two (2) years.

### 4.3. ITA Processing Fees

Initial certification of an ITA carries a Processing Fee which is payable in two instalments as follows:

	1 <sup>st</sup> Instalment	2 <sup>nd</sup> Instalment
<b>Phase:</b>	Stage 1	Stage 2
<b>When:</b>	Concurrently with the submission of ITA Application Form	Concurrently with the submission of the Systems Audit Report
<b>How:</b>	Details provided on the ITA Application Form	Details provided on the Systems Audit Report Submission Form
<b>Amount:</b>	As determined in the Innovative Technology Arrangements and Services (Fees) Regulations	As determined in the Innovative Technology Arrangements and Services (Fees) Regulations

The Stage 1 fee instalment shall be remitted concurrently with the ITA Application Form, in line with the payment details provided on the form. It is important that Applicants follow the remittance instructions provided to avoid processing delays. Payment details are to be included on the ITA Application Form in the respective section.

The Stage 2 fee instalment shall become payable with the submission of the Systems Audit Report Submission Form following the remittance instructions on the form and including payment details in the relative section on the form.

#### 4.4. Documentation Required

Applicants are required to supplement the ITA Application Form with a number of documents as indicated below. The documents required will vary according to the type of Applicant, type of ITA and organisational setup of the Applicant.

Document	Individual	Legal Organisation
1. Valid identification document	✓	
2. Verification of residential address (if not included on identification document)	✓	
3. Fit and Proper Questionnaire of personal Applicant	✓	
4. Explanation of the ownership and control structure		✓
5. Corporate structure chart showing the ownership structure		✓
6. Memorandum and Articles of Association, or equivalent document		✓
7. If directors and shareholders details are not included in the Memorandum and Articles of Association: <ul style="list-style-type: none"> <li>• Directors register, or equivalent document</li> <li>• Shareholders register, or equivalent document</li> </ul>		✓
8. Fit and Proper Questionnaire for every Qualifying Shareholder		✓
9. For every Qualifying Shareholder documents 1 and 2 above, as applicable		✓
10. Business model	✓	✓

Document	Individual	Legal Organisation
11. Blueprint ( <i>refer to Section 6. Specific Requirements below for details</i> )	✓	✓
12. If the Applicant falls under Article 8(5) of the ITAS Act, confirmation by a registered Systems Auditor of the requirements that the ITA is not in compliance with and the technical challenges encountered.	✓	✓
13. Where an Administrator (as defined in Article 2 of the ITAS Act) is appointed, the following must be provided: <ul style="list-style-type: none"> <li>• Valid identification document</li> <li>• Verification of residential address (if not included on identification document)</li> <li>• Fit and Proper Questionnaire</li> </ul>		✓
14. Letter or appointment for every Technical Administrator engaged	✓	✓
15. Where a Resident Agent is appointed, the following must be provided: <ul style="list-style-type: none"> <li>• Valid identification document</li> <li>• Verification of residential address (if not included on identification document)</li> <li>• Fit and Proper Questionnaire</li> </ul>	✓	✓

## 5. General Requirements

In line with Article 8(3) of the ITAS Act, the ITA must satisfy the general requirements intended to meet the standards of:

- **Legality** of the purpose and function of the ITA;
- **Integrity** of the Applicant, including Administrator and Qualifying Shareholders, where applicable;
- **Transparency** of the functions and limitations of the ITA to its users;
- **Compliance** with all applicable legal obligations; and
- **Accountability**, by clearly identifying who will be fulfilling the roles contemplated in the ITAS Act and defining the responsibilities of each individual, particularly in instances where there are multiple appointments.

The Authority will assess all the information provided in the ITA application and will review all documents provided supporting said application in order to reach a conclusion.

## 6. Specific Requirements

In line with Article 8(4) of the ITAS Act, the Authority shall issue an ITA Certification only when the following specific requirements have been met to the satisfaction of the Authority:

- a) fit and properness;
- b) positive assurance from Systems Auditor/s;
- c) appointment of Technical Administrator/s;
- d) compliance with applicable and mandatory law; and
- e) adequate disclosures to users.

### 6.1. Fit and properness

In issuing a certification to an ITA, the Authority will need to ascertain both the fitness and properness of the ITA and the person/s exercising control.

#### Fitness and properness of the ITA

In its review and assessment of an ITA application, the Authority will need to ascertain that the ITA:

- is fit and proper for the purpose/s declared; and
- has the qualities, attributes, features, behaviours or aspects declared.

In this respect, when submitting an application for an ITA certification, Applicants are required to submit a Blueprint to the Authority, which shall include, inter alia, the following information:

Specific Requirements	Typical questions to be answered
<b>Purposes</b> <i>The reasons for which the ITA is being, or was, created.</i>	<ul style="list-style-type: none"><li>• What social or business needs is the ITA trying address (if any)?</li><li>• What benefits are expected to be derived from the ITA?</li></ul>
<b>Qualities</b> <i>The specific characteristics that the ITA offers to its users.</i>	<ul style="list-style-type: none"><li>• What are the specific characteristics that will allow the ITA to achieve its Purposes?</li></ul>
<b>Aspects</b> <i>The specific elements or boundaries of the ITA that are subject to the certification.</i>	<ul style="list-style-type: none"><li>• What are the defined boundaries of the ITA (including activities occurring 'On-Chain' or 'Off-Chain') that are subject to the ITA certification?</li></ul>

Specific Requirements	Typical questions to be answered
	<ul style="list-style-type: none"> <li>• How is the ITA designed from a technical perspective (making reference to the Technology Stack – refer to Appendix III)?</li> </ul>
<p><b>Features</b> <i>The distinctive functional capabilities of the ITA.</i></p>	<ul style="list-style-type: none"> <li>• What are the expected data sources to be used as inputs?</li> <li>• What specific computations, if any, are expected to be carried out ‘On-Chain’?</li> <li>• How will the ITA operate in achieving the specific purposes?</li> <li>• Is the ITA linked to other external systems? If so, how is the ITA interfacing with such systems?</li> <li>• How will the ITA provide functionality to allow the Technical Administrator to exercise the duty to intervene as required in Article 8 of the ITAS Act?</li> <li>• What specific functionality will allow the ITA to meet the obligations of applicable and mandatory law?</li> </ul>
<p><b>Attributes</b> <i>The inherent capabilities of the ITA.</i></p>	<ul style="list-style-type: none"> <li>• What Codebase is being used (open-source, closed-source)?</li> <li>• What element of non-alterability is in place (if at all)? And if so, what is the agreed process for altering the protocol?</li> <li>• What conflict resolutions mechanisms are in place?</li> <li>• How are transactions processed?</li> <li>• How can the network be accessed?</li> <li>• How is data shared within the ITA?</li> </ul>
<p><b>Behaviours</b> <i>The manner how the ITA responds to unexpected processes and inputs.</i></p>	<ul style="list-style-type: none"> <li>• Does the ITA have monitoring and enforcement capabilities to detect and stop fictitious transactions from being recorded?</li> <li>• How will the ITA react to unexpected circumstances? How will the ITA report critical issues to users?</li> <li>• Does the ITA have functionality to identify trends and predict issues beforehand?</li> </ul>

Specific Requirements	Typical questions to be answered
<b>Limitations</b> <i>The technical and/or operational restrictions of the ITA.</i>	<ul style="list-style-type: none"> <li>• Does the ITA have any inherent limitations (such as scaling limitations, low throughput, transactions confirmation speed, etc.)?</li> <li>• What are the reasons, if any, that the ITA is not in position to provide functionality to the Technical Administrator to intervene as required in Article 8 of the ITAS Act?</li> </ul>

The Authority will issue further guidance on the Blueprint, including a proposed template/layout, at a later stage.

The Applicant must ensure that any information included in the Blueprint, the basis of which a user is invited to participate in, rely on or use the ITA, shall be disclosed to the users as outlined below in Section '6.5 Adequate disclosures to users'.

In addition, the Applicant must ensure that the ITA is implemented in line with the submitted Blueprint, as this document will serve as the basis for the Systems Audit as outlined below in Section '6.2 Positive assurance from Systems Auditor/s'.

### **Fitness and properness of the Applicant**

The individual and/or legal organisation, in the name of which an application for an ITA certification is submitted to the Authority, shall be required to be fit and proper at all times. Specifically, as required in Article 8(4)(a) of the ITAS Act, in the case where the Applicant is a legal organisation, the Applicant shall ensure that:

- an appointed Administrator of the legal organisation, if any, is fit and proper to carry out the functions of an administrator (refer to Appendix I for more detail); and
- any Qualifying Shareholder (refer to Appendix II for more detail) of the legal organisation is a fit and proper person.

In order to enable the Authority to determine the fitness and properness of these individuals, each individual that meets the above criteria is required to submit a 'Fit and Proper Questionnaire' to the Authority as part of the ITA Application Form.

Moreover, the Applicant must also provide the MDIA with a business model and demonstrate how the service or technology shall be sustainably financed.

## 6.2. Positive assurance from Systems Auditor/s

Upon successful completion of Stage 1 of the application process, the Authority will issue a Letter of Intent and inform the Applicant to proceed with the appointment of a Systems Auditor. In line with Article 8(4)(b) of the ITAS Act, the Systems Auditor is required to provide the Authority with an opinion on whether the ITA meets reasonable standards as set out by the Authority, which, inter alia, shall include:

- the specific purposes, qualities, features, attributes, behaviours or aspects of the ITA as declared in the Blueprint;
- where applicable, authorisations or powers granted to the Authority, Lead Authority, Technical Administrator or the ITA itself; and
- compliance with any rules and regulations made under the ITAS Act and any guidelines issued by the Authority, as well as any conditions established by the Authority in the particular case.

The Authority will indicate the type of Systems Audit that is required as part of Stage 2 of the application process. Details on the different types of Systems Audits and standards to be met are included in Chapter 1 of the MDIA Guidance Notes. However, it is important that Applicants are aware of the different types of Systems Audits and the frequency of Audit the Authority has set out.

In the case of non-operative ITAs (i.e. ITAs that, at the time of application for an ITA certification, are not yet live or have been operating for less than six (6) months), the Authority shall initially require a Type 1 Systems Audit to be conducted. If the Authority, following the Type 1 Systems Audit, issues an ITA certification, the Applicant will be then required to undergo a Systems Audit for compliance purposes. In this regard, a Type 2 Systems Audit will be required following 6 months from the ITA Go Live date. Thereafter, a Type 2 Systems Audit shall be required on an annual basis.

On the other hand, in case of operative ITAs (i.e. ITAs that, at the time of application for an ITA certification, are live and have been operating for at least six (6) months), the Authority shall request a Type 2 Systems Audit. Thereafter, the ITA shall undergo a Type 2 Systems Audit on an annual basis.

Upon receipt of the Systems Audit Report the Applicant shall complete and submit the Systems Audit Report Submission Form to the Authority.

Applicants need to take note of the following times frames for completion of Systems Audits:

	Systems Audit Type	Initiation of Systems Audit	Report submitted to MDIA
Non-operative ITA	Type 1 <i>(Stage 2 of Application Process)</i>	At any point in time following MDIA's Letter of Intent.	Within 3 months from the Systems Auditor Green Light* issued by the Authority.
	Type 2 <i>(First Type 2 following Certification)</i>	Within six (6) months from Go Live date.	
	Type 2 <i>(Annual)</i>	After twelve (12) months from the period-end of the latest Type 2 Systems Audit.	
Operative ITA	Type 2 <i>(Stage 2 of Application Process)</i>	At any point in time following MDIA's Letter of Intent	Within 3 months from Systems Auditor Green Light* issued by the Authority.
	Type 2 <i>(Annual)</i>	After twelve (12) months from the period-end of the latest Type 2 Systems Audit.	

*\* The Systems Auditor must notify the MDIA upon engagement by the Applicant (refer to Chapter 1 Section 7 – Systems Auditor Guidelines). The MDIA will issue the Green Light to the Systems Auditor to commence the Systems Audit once it is satisfied that the Systems Auditor is competent to audit the respective ITA.*

### 6.3. Appointment of Technical Administrator/s

An ITA shall have a Technical Administrator, registered with the Authority, in office at all times. An ITA may have more than one Technical Administrator appointed. Details of the Technical Administrator/s appointed shall be provided as part of the ITA Application Form.

In considering the application for an ITA certification, the Authority will need to ascertain that the appointed Technical Administrator/s is/are registered with the Authority and can fulfil their duties and responsibilities with respect to the ITA being certified. Specifically, in line with Article 8(4)(c) of the ITAS Act, the Technical Administrator shall demonstrate to the Authority that the ITA is able to:

- satisfy all pre-requisites for the certification which may be granted to it under this Act;

- meet standards on a continuing basis and to address critical matters, and how to address them, as are stated in Guidelines, if any, by the Authority in the event they occur;
- vary parameters or functionalities where the objective of the system is to address mandatory legal requirements which may reasonably be predicted to change over time; and
- with reference to matters, if any, upon which, the Technical Administrator; the Authority or Lead Authority; or any other designated person, may be given the discretion or may be required to intervene and which are addressed by the software, all authorisations or powers required to carry out such interventions exist and operate as intended.

In addition, Article 8(4)(d)(iii) of the ITAS Act requires that ITAs shall have in-built technology features, to enable the Technical Administrator, to intervene in a transparent and effective manner in the event of:

- a) a material cause of loss to any user; or
- b) a material breach of law,

so as to ensure that the cause of loss or breach of law is satisfactorily addressed to the best of his/her abilities and to ensure it does not occur or re-occur, and in case of unjustifiable failure by the Technical Administrator, on the intervention of the Authority.

*However, the Authority acknowledges that, in specific ITA implementations, the functionality to grant the Technical Administrator and the Authority, where applicable, power to intervene, as required in Article 8(4)(c)(iv) and Article 8(4)(d)(iii) of the ITAS Act, may not be technically feasible or justifiable. In this regard, when it is clearly justified as to why the implementation of such functionality cannot be achieved, the Authority reserves the right to vary this requirement. In doing so, subject to all other requirements being successfully met by the Applicant, the Authority may issue an ITA certification that clearly states that the requirements of Article 8(4)(c)(iv) and Article 8(4)(d)(iii) of the ITAS Act are not being met. In addition, the Applicant shall be required to disclose such limitation to all users as part of the Terms of Service.*

Further details on the eligibility criteria and duties of the Technical Administrator is included in Chapter 3 'Technical Administrator Guidelines' of the MDIA Guidance Notes.

#### 6.4. Compliance with applicable and mandatory law

As required by Articles 8(4)(d)(i) and 8(4)(d)(ii) of the ITAS Act, the Applicant needs to demonstrate to the Authority how the ITA will meet obligations imposed upon it by applicable and mandatory law, including but not limited to, those relating to:

- a) the prevention of money laundering and the financing of terrorism;
- b) the protection of personal data,
- c) the respect of the rights of consumers; and
- d) other mandatory laws, depending on the purpose and functionalities of the ITA.

In submitting an application for an ITA certification, the Applicant shall clearly indicate whether these obligations will be met by implementing physical/manual procedures outside the ITA boundaries or through in-built functionalities within the ITA. In the case of the latter, the Blueprint shall clearly indicate these functionalities. In addition, in the case where the Applicant states that any mandatory law is not applicable, the Applicant is also required to provide justification as to why such requirements do not apply. This information will be reviewed by the Authority as part of Stage 1 of the application process, and the Applicant may be requested to provide additional information or clarifications.

The Applicant is responsible for ensuring that the procedures implemented to meet obligations with applicable and mandatory law, as indicated by the Applicant in the application for an ITA certification, shall be in line with any guidance issued by the Lead Authority on the respective subject, and which may be updated from time to time.

#### 6.5 Adequate disclosures to users

The Applicant must ensure that the specific purposes, qualities, features, attributes, limitations, conditions, terms of service and behaviours or aspects of the ITA, the basis of which a user is invited to participate in, rely on or use the ITA, shall be adequately disclosed to all users or prospective users. Specifically, Article 8(4)(e) of the ITAS Act requires that such disclosures are made in the English language and are in an easily accessible and intelligible format.

Where the Applicant wishes to use multiple languages for this purpose, in case of conflict between languages, the English language version shall prevail. In addition, in the case of conflict between the English language and the underlying code of the innovative technology arrangement, the English language shall prevail.

## 7. Resident Agent

In line with Article 15 of the ITAS Act, an Applicant that is not ordinarily resident in Malta is required to appoint a Resident Agent. Details of the appointed Resident Agent shall be provided to the Authority as part of the application for ITA certification.

Refer to Chapter 4 'Resident Agent Guidelines' issued by the Authority for further guidance.

## 8. Outsourcing

The Applicant may need to outsource some functions in view of resource constraints. In granting a certification, the MDIA must be made aware of material functions that are being outsourced.

Material functions are those functions that are fundamental for the ITA to meet the generic and specific requirements under Article 8 of the ITAS Act. In this respect the Applicant needs to demonstrate to the Authority how the process to operate the ITA will be managed and by whom.

The Authority reserves the right to request copies of outsourcing agreements.

The Authority may also, from time to time issue standards in this respect, which shall be binding on the ITAs seeking certification from the Authority and are eventually certified by the MDIA.

## 9. Certification

### 9.1. Full certification

Upon satisfactory conclusion of the application process, the MDIA will proceed to issue a certificate to the ITA stating the qualities, features, attributes, behaviours and aspect of the arrangement.

In line with Article 8(8) of the ITAS Act, in cases where the ITA is held within a legal organisation, whether with legal personality or not, the certification shall be made in name of the legal organisation. In case of applications in the name of individuals the certificate shall be issued in name of the Applicant and if so requested, also in the name of the Technical Administrator.

In line with Article 8(6) of the ITAS Act, the Authority shall also enter the name of the certified ITA on the Register of recognised innovative technology arrangements, under the applicable category.

### 9.2. Conditional certification

In the case of:

- a) DLTs or other ITAs which are in operation, or at a very advanced stage of development the date the ITAS Act come into force; and
- b) open, decentralised, public and permission-less DLTs, and other similar ITAs,

where compliance with one of the requirements for certification of an ITA stated in Article 8 of the ITAS Act is not practicable within short time frames due to technical challenges, may still submit an application for certification by the MDIA subject to a number of conditions:

- a) a Systems Auditor (recognised by the Authority) and confirmed by the Authority that he/she can audit such ITA, must confirm what the shortcomings are, the technical challenges encountered and the reason why these cannot be implemented in a short time scale; and
- b) the Authority together with the Applicant shall identify:
  - i. the issues on which there is non-compliance with the legal requirements stated in Article 8 of the ITAS;
  - ii. the matters which need to be overcome for such issues to be addressed;
  - iii. the manner in which such issues may be addressed as would satisfy the Authority of compliance with said Article; and

- iv. the time frame within which the issues are to be addressed.

Based on the above the Authority may proceed to issue a Conditional Certificate to an ITA in these circumstances.

The ITA will have to comply with all the requirements of Article 8 within the time frames agreed. In addition a Systems Auditor (recognised by the MDIA) will need to issue a positive assurance that the necessary actions and modifications have been made to the ITA to achieve the agreed outcomes and compliance.

The condition shall be recorded in the certification and subsequently the register for recognised innovative technology arrangements held by the MDIA.

## 10. Ongoing obligations

### 10.1. Display of certificate

Once certification process is completed successfully, an ITA shall be granted a Certificate under the ITAS Act. The Certificate will state the details of how the ITA shall be identified, including any public key or a brand name. The Certificate will carry a unique number for purposes of identification.

The Certified ITA shall post the Certificate on the arrangement, in a specific location which shall be notified to the Authority, in an easily accessible and legible format so it can be viewed and understood by all users of the ITA.

### 10.2. Go Live Date

Once the Authority certifies a non-operative ITA, it is expected that it goes live within the time frame indicated in the ITA Application Form.

If, for any reason the Certified ITA is not in a position to comply with this condition, it shall notify the Authority in writing setting out the reason/s for such a delay together with a revised expected Go Live date.

Should the Certified ITA not manage to achieve a Go Live date within 12 months from date of Certification, the Authority reserves the right to suspend the Certification pending further developments from the ITA.

### 10.3. Material Changes

In the event of any material changes, the Certified ITA is obliged to engage with the Authority to either obtain the Authority's prior approval to the change or notify the Authority of the change as further explained below.

Where the Certified ITA needs to notify the Authority of a material change, such notification shall be made to the Authority formally, in a durable medium. The request to notify the Authority of a change shall not be satisfied merely by the fact that the information which ought to be notified to the Authority is included in a standard annual return.

For the purpose of these ongoing obligations, "material changes" with reference to an ITA arrangement shall include:

- a) any alternations of any of the software on which an assurance has been provided by a Systems Auditor;
- b) any development altering the rights of users;

- c) any development altering the rights, authorisation and powers of the technical administrator or the Authority;
- d) any change in the Technical Administrator;
- e) any change in an administrator of a relevant legal organisation;
- f) any change in a Qualifying Shareholder; and
- g) any change in the person with reference to whom a certification has been issued.

#### 10.4. Prior approval of the Authority

The following material changes require the Certified ITA to provide the Authority all the relevant details, as well as, any applicable fees, prior to the changes taking place:

- a) any change in the Technical Administrator;
- b) any change in an Administrator of a relevant legal organisation;
- c) any change in a Qualifying Shareholder; and
- d) any change in the person with reference to whom a certification has been issued.

The Authority shall review the proposed changes and following its assessment the Authority will communicate outcome to the Applicant.

Additionally, if the Certified ITA effects any of the following changes and cannot provide a confirmation by a Systems Auditor (recognised by the MDIA) that such changes do not impact the last Systems Audit Opinion issued on the ITA, then such changes will require the prior approval of the MDIA:

- a) any alternations of any of the software on which an assurance has been provided by a Systems Auditor;
- b) any development altering the rights of users; and
- c) any development altering the rights, authorisation and powers of the technical administrator or the Authority.

#### 10.5. Notification to the Authority

In the following instances, the Certified ITA must provide the Authority with the particulars of the change, as well as, any applicable fees, within thirty (30) days of such changes:

- a) any alterations of any of the software on which an assurance has been provided by a Systems Auditor;
- b) any development altering the rights of users; and
- c) any development altering the rights, authorisation and powers of the technical administrator or the Authority.

Notification of these changes will suffice as long as, a Systems Auditor (recognised by the MDIA) confirms that such changes do not impact on the last Systems Audit Opinion issued on the ITA.

## 11. Renewal process

A Certified ITA seeking renewal of its certification must submit an ITA Certification Renewal Form to the Authority, three (3) months prior to the expiration of the current certification, together with the applicable fees.

## Appendix I - Who is the Administrator?

In line with the Fourth Schedule of the ITAS Act, an Administrator means an officer or any person who is appointed to carry out representative and fiduciary functions in the control and administration of a legal organisation, and any person who carries out such functions even if under another name but shall not include a Technical Administrator or a Resident Agent under the ITAS Act or a VFA agent under the Virtual Financial Assets Act, 2018, and the term "board of administrators" shall be construed accordingly.

The term Administrator shall not include any user who has the right or power to express his views or consent to a proposal in relation to the software consisting of an ITA when such user is a member of the user community and his holding or functions do not permit him to influence decisions on his own. Having said this, a user shall be considered to be in a position to influence decisions as an Administrator if he holds a post within the organisation which enables him to vote with a weighting of more than 25% in favour of or against material decisions relating to the governance of the arrangement.

For avoidance of doubt, Administrator shall mean:

- a) a person who has powers of representation and may generally bind the legal organisation in contract;
- b) a person who has control of assets belonging to the legal organisation and who has any powers in relation to the assets of any user which may be using the arrangement;
- c) a person who has supervisory functions over the operation of the software and may intervene in the normal course of business to respond to queries by the users, in particular for access to the software, access to and powers to amend documentation evidencing the terms and conditions applicable to participation on the arrangement, taking decisions relating to on-boarding of persons onto the arrangement, decisions on the application of mandatory laws and generally on changes relating to the software itself when prompted by the market in which it operates, the Technical Administrator or the Authority, including taking final decisions on proposed reorganisation or forks of the arrangement, and in such cases whoever has the power to decide which underlying blockchain or DLT software to use; and
- d) a person having general governance functions in relation to the arrangement, duties under any rules of an exchange, duties of compliance

with any mandatory laws applicable to the context and other fiduciary obligations listed in article 1124A of the Civil Code<sup>1</sup>.

---

<sup>1</sup> Chapter 16 of the Laws of Malta

## Appendix II - Who are the Qualifying Shareholders?

In line with the Fourth Schedule of the ITAS Act, the term Qualifying Shareholder includes any shareholder who:

- owns or controls the ITA;
- holds more than 25% of the shares or ownership interests in the legal organisation; or
- through provisions of the statute, has special voting or other rights permitting him to exercise effective control over the activities of the legal organisation.

Where in any particular case and on analysis of an arrangement it is not possible for any person to be identified as falling within the above categories, then the Authority shall proceed on the basis that there are none and may

- tailor the conditions of recognition to such context; or
- require that reference be made to any other person who may be providing material operational services to the ITA or who may be receiving material economic benefit from the operations of the arrangement.

For the avoidance of doubt, the term 'shareholder':

- a) shall include any holder of shares in a company, any partner in a partnership, any beneficiary under a foundation or any other member in a co-operative or association of persons who has a share in the capital or a share in the profits of the legal organisation, and who may vote on general matters raised for the holders thereof to express their view;
- b) shall refer to persons who have the power to vote on a proposal to amend the software or architecture of an ITA which can modify the rights of the holders thereof other than on inconsequential administrative aspects;
- c) only includes a holder of tokens whether issued with reference to the specific innovative technology arrangement or otherwise, which:
  - i. are issued by a legal organisation with reference to an ITA and which grants such rights to the holder thereof with the intention of reflecting the same status and powers in the legal organisation which owns the ITA; or
  - ii. qualify as "equity" in the legal organisation or the arrangement, in that they give the holder thereof a share in the capital and profits of, or in relation to, the arrangement and voting powers in relation to

an ITA and which enable him to vote in favour of material decisions relating to defined matters established for the continuing operations of the arrangement and has:

- A. a weighting of more than 25% of the total tokens in issue;
- B. under reserved powers, a veto or similar power where he may determine the outcome of a vote or a proposal due to special rights vested in him notwithstanding that he may hold less than 25%, and shall not include any other user or owner of tokens or other digital assets even if they have a voting right, a right to be granted additional tokens in specified circumstances or any other power or right to participate in specified circumstances.

## Appendix III – Technology Stack and Use Cases

This Appendix aims to provide further insight in regards to the various components which a DLT solution may comprise of at the most generic level.

### Further definitions from the applicable Acts

For ease of reference the definitions as per the current MDIA and ITAS acts are listed here:

"innovative technology arrangements" 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;

"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, and the term "node" means a device and data point on a computer network;

"smart contract" 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;

### Technology Stack

A DLT platform, from an abstract view, provides a method for distributed nodes which:

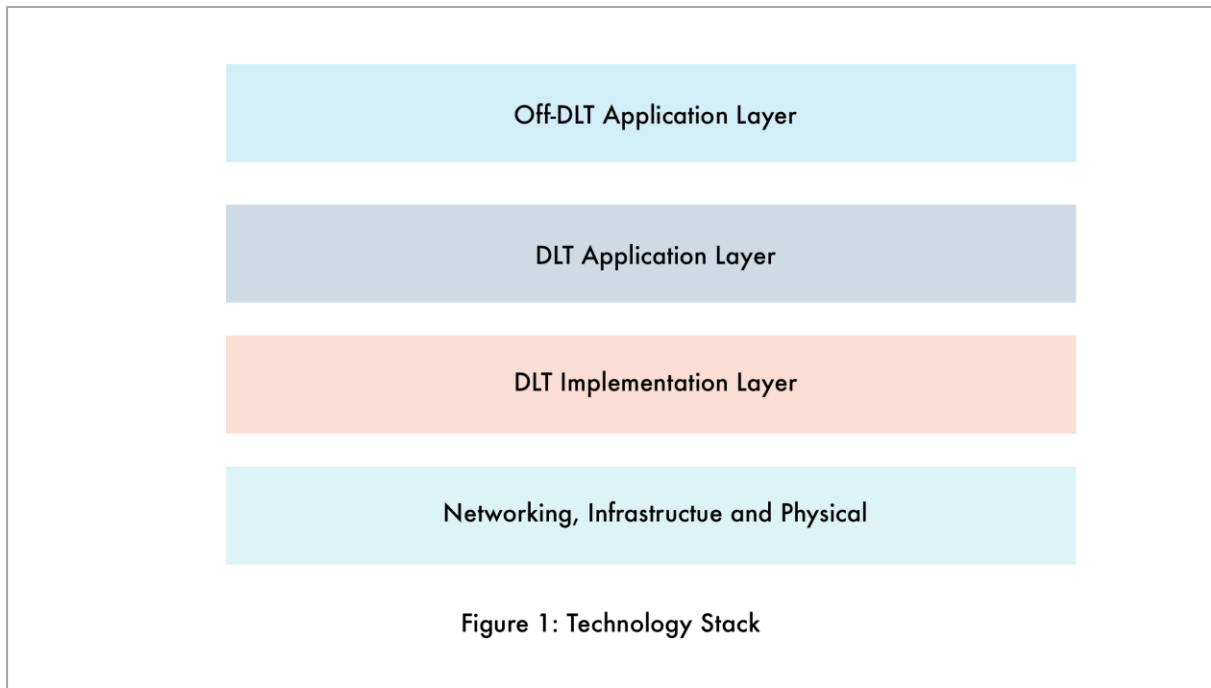
- (i) do not inherently trust each other; and
- (ii) cannot necessarily communicate with all other nodes;

to provide for the execution of system logic without a central authority.

Blockchain was the first implementation of a DLT, however since it was first proposed other methods to implement a DLT have been proposed. Therefore, no reference will be made to any specific implementation and neither to

implementation specific algorithms (e.g. using Proof-of-Work, Proof-of-Stake, etc), but a generic description of what a DLT is to encapsulate different implementations will be used.

An abstract technology stack is depicted Figure 1.



Networking, Infrastructure and Physical Layer: This layer consists of all hardware, software and networking protocols which are not part of the DLT implementation, yet on which the DLT implementation runs on top of. As an example, this may include TCP/IP protocols, hardware network interfaces, routers and other networking infrastructure. Whilst a DLT implementation Applicant may not necessarily have access to and/or have influence on the design and implementation of this layer, the Applicant should be well informed of the various components used in this layer which it makes use of and the implications of how such components may affect the DLT platform.

DLT Implementation Layer: The DLT implementation layer is that system logic, typically encoded within a DLT node software application, that enables distributed nodes to interact and work together in a decentralised manner to provide the trust guarantees proposed. This may include a number of components included but not limited to network access and node discovery, validation, conflict resolution, incentivisation, an application execution environment, governance mechanisms, a means of consensus and any other code or logic that is required to implement and provide the DLT platform.

*DLT Application Layer*: Many DLT implementations allow for application logic to be executed on top of the platform, ensuring decentralised code execution. This application logic is separate to and executes on top of the *DLT Implementation Layer*. Such application logic does/may not require knowledge of the lower level *DLT Implementation Layer* (e.g. such code does not have visibility of the fact that it is being executed on a number of DLT nodes in a decentralised manner). This layer could allow for applications to be loaded by users who may not necessarily be developers of or run a participating node within the *DLT Implementation Layer* on which it is meant to execute. The application logic which this layer encapsulates is often termed *Smart Contracts* (e.g. Solidity Smart Contracts which execute on Ethereum), *Scripts* (e.g. Bitcoin Script) and *Chaincode* (e.g. Hyperledger Chaincode). For the purpose of disambiguation, irrespective of commonly used terms, the *DLT Application Layer* is defined by that code which executes on top of the *DLT Implementation Layer* which allows for trusted execution of applications (which are not necessarily part of the DLT Implementation).

*Off-DLT Application Layer*: The DLT trusted environment which the *DLT Implementation Layer* provides is limited to the *DLT Application Layer* executing on top of the DLT platform. As soon as any interaction is required from outside the *DLT Application Layer*, such trusts that the DLT platform provide are gone. The *Off-DLT Application Layer* encapsulates all logic that executes outside of the DLT platform. For example, web pages that are served from outside of the DLT which provide users with services to interact with the DLT platform and/or DLT Application is considered to be Off-DLT Application logic.

## Variations and Hybrids

Since the introduction of Bitcoin and Blockchain systems, many different variations of DLT implementations have been proposed. It is for this reason that the stack above is a generic one, so as to encompass different DLT platform variations and hybrids - irrespective of whether they are public, private, permissioned; use Proof-of-Work, Proof-of-Stake, or any other consensus mechanism; whether some guarantees are provided in a hybrid manner (e.g. zero-knowledge proofs); or any other variation thereof.

## Boundaries, Dependencies and Interfaces

When describing the innovative technology arrangement (ITA) it is important to define:

- (i) the boundaries of the ITA, i.e the parts of the ITA that fall within a specific layer or across different technology stack layers;

- (ii) any dependencies which the ITA relies on and the implications of such dependencies; and
- (iii) the interfaces which each layer will expose for use by other layers or users (whereby users could also be other computational systems).

## Use Cases

The following ITA use cases are provided for exemplification:

1. Consider a merchant that wants to provide a guarantee to clients that 10% of the amount they pay to the merchant, will immediately and automatically go to a particular charity. This is the only functionality coded within the Smart Contract - a function that can receive funds and automatically send 10% of the funds to the charity, and the remaining 90% to the merchant's wallet. The merchant creates a Smart Contract that provides for this functionality. In this case the Smart Contract in its entirety is the ITA.

With respect to the technology stack, the whole ITA (i.e. the Smart Contract) falls squarely in the *DLT Application Layer* and this defines the ITA's boundaries. The ITA, being a Smart Contract, is dependent on the *DLT Implementation Layer* on which it executes.

The Applicant must demonstrate sufficient understanding and provide sufficient detail and links to resources which describe the underlying *DLT Implementation Layer* including but not limited to its operation, its consensus mechanisms, identification of any points of centralisation, and any other detail pertaining to how the platform may affect the *DLT Application Layer*.

The Authority may request further clarification and details where required. The interface which the ITA (i.e. the Smart Contract) exposes are the functions that can be called from the outside world - in this case it is the 'receive funds' function. This interface may allow for software within the *Off-DLT Application Layer* or for users to interact directly with the Smart Contract.

2. Consider an application for a Blockchain platform that supports uploading and execution of user defined smart contracts. The Blockchain platform allows for decentralised nodes to communicate over the Internet using TCP/IP protocols. The ITA in its entirety is the Blockchain platform. This ITA

is defined within the *DLT Implementation Layer* which also clearly outlines the associated boundaries.

The Applicant should provide sufficient detail including but not limited to: how the ITA, i.e. the Blockchain system, is implemented and sufficient description of the algorithms used which achieve consensus, identification of any points of centralisation, descriptions pertaining to the smart contract execution engine (which may be a virtual machine), the level of transparency of data (or even non-transparency), how immutability is achieved, security features, and any other algorithms or protocols that define the Blockchain platform.

The Blockchain platform, that is the ITA, is dependent on the underlying Internet infrastructure. The ITA (the Blockchain platform), provides an interface (an Application Programming Interface, API) by which smart contracts (in the *DLT Application Layer*) need to abide by in order to execute on the platform. The Blockchain platform may also expose an interface which allows users (including computational systems) to make calls to functions exposed by smart contracts (in the *DLT Application Layer*). Any such APIs or interfaces need to be described sufficiently within the application.



[mdia.gov.mt](https://mdia.gov.mt)