Forensic Node Guidelines

MDIA
Malta Digital Innovation Authority

Forensic Node 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.

changes in Version 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. As an example, in the case of an issuer of a VFA, the Whitepaper, or parts thereof, registered with MFSA shall serve as the Blueprint. Further information on the contents of the Blueprint is provided in Chapter 2 of the MDIA Guidance Notes.

"Innovative Technology Arrangement", also referred to as "ITA" within this document, is 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.

"ITAS Act" refers to the Innovative Technology Arrangements and Services Act, 2018.

"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 technology arrangement.

"Systems Auditor" ('SA') as defined in the Innovative Technology Arrangements and Services Act, 2018.

"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.

"Node", for the scope of this document, is in reference to the Forensic Node. The term 'node' is hereby used in the wider sense of a machine connected to the rest of the system and is not to be conflated with, or limited to, the narrower notion of a DLT node.

2 Purpose of this Document

The MDIA provides a certification process for Innovative Technology Arrangements (ITAs), which certification indicates dependability of the ITA from a technological perspective. In order to qualify for certification, MDIA-licenced Systems Auditors must attest to the fidelity of the ITA with respect to the functionality specified in the ITA blueprint, and that the ITA has all the necessary components to ensure that all the necessary information is stored and synchronized in real-time in order to allow for continued assessment of the ITA and to allow for investigations if required at a later stage. In order to achieve this, ITAs must include a Forensic Node which is used to keep a trail of behaviour on the ITA as a whole. If the creation and upkeep of a Forensic Node is not feasible in technical terms, technical reasons why this requirement cannot be met need to be provided to the MDIA and the applicant must find an alternate technical arrangement acceptable to the MDIA wherein all necessary ITA information is stored and synchronized in the Maltese Jurisdiction in real-time and in a tamper-proof manner.

The aim of this document is to specify the requirements of such a Forensic Node, which may vary from one ITA to another, depending on the ITA's functionality. This document should act as guidelines to ITA certification applicants as to what are the minimal guarantees to be provided in their Forensic Node and for the Systems Auditors in order to be able to evaluate the adequacy of the infrastructure proposed in an ITA's blueprint. This document builds upon previous guidelines issued by the MDIA in respect of the Forensic Node (ITA Blueprint Guidelines section 2.4).

Given that the functionality of ITAs may vary widely, whether it is in terms of what sort of transactions are handled, data handled, etc., the infrastructural requirements on the Forensic Node may vary. However, the role and purpose of the Forensic Node remains the same.

2.1 Overall purpose of the Forensic Node

The aim of the Forensic Node is to store all relevant information on the runtime behaviour of the ITA in real-time including but not limited to transactions carried on the DLT-components of the ITA. Since parts of an ITA may include an Off-DLT Application Layer (see the MDIA **Technology Stack Nomenclature** guidelines), any relevant information and events relevant and accessible to the ITA on this layer (e.g. relevant interaction with the front-end, information stored on an off-chain database core to the ongoing ITA functionality) is also to be stored on the Forensic Node.

Note that due to the all-encompassing and possibly sensitive and/or personal nature of the information to be stored on the Forensic Node, there is no requirement for it to be a DLT node or to reside on a DLT.

The purpose of retainment of this information is for certification purposes, in order to ensure that an audit trail of the system runtime behaviour is stored a faithful manner in order to ensure that:

(i) sufficient information is available to enable Type 2 System Audits (see the MDIA **Systems Auditor Guidelines** and **Systems Auditor Report Guidelines**) to assess operating effectiveness of the controls;

(ii) any request for information regarding legal compliance and the operational behaviour of the system by the MDIA or any other national lead Authority concerned with the functionality of the ITA can be acted upon satisfactorily by the Technical Administrator; and

(iii) sufficient information is available to enable the Technical Administrator to intervene in the case of unexpected behaviour leading to material cause of loss to any user or a material breach of the law as specified in Article 8 of the ITAS Act.

2.2 Achieving the purpose of the Forensic Node

In order to achieve the purpose of the Forensic Node, it must be an essential part of the infrastructure to ensure an audit trail of all relevant ITA and ancillary events and data such that:

(i) All relevant events and data are recorded faithfully in real-time on the Forensic Node without risk of omission or corruption;

(ii) Information is written in a manner to ensure access to the information stored in a tamper-proof and accurate manner that is guaranteed to be faithful to the originally recorded information, that is ensuring that no data or information may be deleted or changed;

(iii) Processes are in place to ensure timely access to this information by the Technical Administrator in a manner that can be demonstrated to be faithful to the original events and data which were recorded on the Forensic Node.

3 Requirements on the Forensic Node

The manner in which the ITA will satisfy the requirements and purposes of the Forensic Node will vary depending on the ITA functionality. However, there are practical requirements which are to be met by the Forensic Node under all circumstances:

- The Forensic Node must be wholly based in Malta in a tier 3[1] or above data centre and must be at all times accessible to the Technical Administrator of the ITA; and

- There need to be documented procedures detailing how the Technical Administrator has access to the data stored on the Forensic Node, including access to the keys in case the data stored on the Forensic Node is in encrypted form and how access shall be granted by the Technical Administrator to relevant authorities and, or law enforcement agencies upon order or request.

The manner in which the purposes of the Forensic Node are to be achieved are to be documented in the ITA Blueprint, including:

- Clear identification of the datasets and events which will be collected and retained on the Forensic Node, including the justification of why the same need to be collected and retained. An acceptable justification is also necessary if any such datasets and events will not be retained on the Forensic Node.

- Clear description of the security measures and mechanisms in place to ensure that data and events stored in the Forensic Node cannot be tampered with and to ensure appropriate protection against unauthorised or unlawful processing or loss of data.

- Data retention policies justifying the storage, deletion and access parameters of the Forensic Node in order to ensure compliance with applicable laws, including data protection laws. This is to include security and access control considerations to ensure legal compliance.

- Detailed documentation of how the purpose of a Forensic Node as defined in this document is achieved by the Forensic Node and ITA infrastructure.

- Clear information on the physical aspects of the Forensic Node, including location of the node and the hardware used.

[1] MDIA is expecting 'Tier 3 Data Centre Qualities' of such a data centre. It need not be a certified tier 3 data centre, but one that conforms to the expectations of such, to the satisfaction of the respective assigned ITA Systems Auditor. Tier classification definitions can be based on Uptime Institute Standards or equivalent.

- Access control procedures in place to ensure that only the Technical Administrator can access information and intervene when legally bound to do so and that the Technical Administrator can grant direct access to relevant authorities and law enforcement agencies if necessary.

As part of the Systems Audit, the Systems Auditors are required to review this documentation in order to ensure compliance with these guidelines and any other legal requirements arising from other guidelines and legislation.