Alastria T Network Operation and Government Policies

v.1.0

Document Control

Version history

Version	Date	Comments
0.1	15-Feb-2019	Initial version using reference to a previous document created by Jesús Ruiz and the Resilience Commission
0.2	19-May-2019	Inclusion of the Acceptance Document section of the Commitment to Execute Critical Nodes
0.3	22-May-2019	Inclusion of the Acceptance Document section of the Commitment to Execute Regular Nodes
0.4	31-May-2019	Minor changes
0.5	23-Sep-2019	Inclusion of standard document references
0.6	25-Sep-2019	Recasting of the three previously existing Policy documents into one and adding of comments from the Core Team and several other reviewers
0.7	03-Oct-2019	Review with Javier Ibáñez to incorporate clarifications of the comments made by Moisés
0.8	07-Oct-2019	Incorporate comments by Domingo Gaitero in reference to the ISO 27001 standards and references to the Intellectual Property Policies in the Statute; and those of Julio San José, small references of NTP and of key guard.
0.9	18-Nov-2019	Update according to suggestions from the last Board of Directors (CML and JLG)
1.0	04-Feb-2020	Changes suggested by Ismael Arribas in relation to terms in the Glossary and sections of the rest of the policy
1.01	04-Mar-2020	Inclusion of a clarification in section 3.1.2 “This point of free reading access does NOT occur in the case of the Alastria Partner Node T Network as specified below.”

Issue Control

Owner: Juan Luis Gozalo

Reviewed by:

Miguel García - Alastria CPO - Date: 27/Sep/2019

Jaime Cuesta - Alastria Project Manager- Date: 27/Sep/2019

Cristina Martínez - Alastria CLO - Date: 27/Sep/2019- 22/October/2019 Carlos Pastor - Identity Commission Leader - Date: 27/Sep/2019

Nacho de la Vega - Identity Core and Platform Core Team - Date: 27/Sep/2019 Urko Larrañaga - Platform Core Team - Date: 27/Sep/2019

Nacho Alamillo - Standards Commission Leader - Date: 30/Sep/2019

Ismael Arribas - Standards Commission Leader - Date: 30/Sep/2019, Dec/2019 Javier Ibáñez - CITT Sponsor - Dates: 21/Sep/2019, 11/Oct/2019
Julio San José - Resilience Commission Leader - Date: 07-Oct/2019
Domingo Gaitero - Social Process - Quality Expert - Date: 07/Oct/2019 Legal Committee: Date: 17/Oct/2019
Legal Committee: Date: 21/Nov/2019

Approved by: Board of Directors 28/Nov/2019
Legal Committee: 21/Nov/2019

Distribution: None

File reference:

Change Log

Version	Status[1]	Changes on version
0.1	JLG	Initial Version
0.2	JLG	Inclusion of the Acceptance Document section of the Commitment to Execute Critical Nodes
0.3	JLG	Inclusion of the Acceptance Document section of the Commitment to Execute Regular Nodes
0.4	JLG	Delete the word Telsius from section 2
0.5	JLG	Incorporate references to terms, policies and definitions throughout the text. Rewriting of the Permitting Policy sections and include De-Permitting
0.6	JLG	Recast: This document now incorporates the Permitting Policy, the Critical Node Policy and the Regular Node Policy, all in one document. Also changing "Alastria Network" to "Alastria Partner T Network" Including references to the Emergency Committee and to the Incident and Change Policies
0.6	NdLV	Clarifications on the permitting and Bootnodes
0.6	IA, CML, MG, JC, CP	Clarification T Network the base software "es" of the Quorum software, also indicating that the Alastria Partner work teams have made the corresponding modifications to this software. Glossary Changes Correction on pg. 17 on definition

[1] Juan Luis Gozalo (JLG); NdLV (Nacho de la Vega); IA (Ismael Arribas); NA (Nacho Alamillo); CML (Cristina Martínez Laburta); MG (Miguel García); JC (Jaime Cuesta), CP (Carlos Pastor); JI (Javier Ibáñez); JSJ (Julio San José); DG (Domingo Gaitero)

		Changes to the T Network topology charts to give more clarity Clarification of network type assigned to T Network according to ITU Change from "organizational" to "organizing" and "operational" Unite the Glossary sections into a single one
0.7	JLG/JI	Incorporate clarifications based on the comments received from Moises to make clear responsibilities and statement of the “Best Effort” Network
0.8	JSJ, DG	Change NTP from nis.org to hora.roa.es Clarify where the keys of the nodes are kept Incorporate footnote of alignment with ISO 27001 Incorporate footnote of reference to Intellectual Property Incorporate footnote of reference to Data Privacy/GRPD
0.9	CML, JLG	Inclusion of sections 9.1 and 9.2 Setting the table of contents and section format Eliminate the specification of "mandatory" in several sections replacing it with "strong recommendation".
1.0	IM, CML, JLG	Precision of terminology in the glossary and in different sections according to IM comments.
1.01.	JLG, CML	Inclusion of a clarification in section 3.1.2 “This point of free reading access does NOT occur in the case of the Alastria Partner Node T Network as specified below.”

Contents

Glossary

Associate: member of the Alastria Network Consortium Association.

AWS - Amazon Web Services: Virtual infrastructure machine service provider to host web services, processing, etc...

Systems bastion (or hardening): set of security policies, hardening and clear delimitation of the privileges of users, groups, roles and configuration of internet protocol services (*Internet Protocol*, IP)[2].

CPD (Data Processing Centre): Physical location where the physical machines are installed where computer operations are processed.

DLT (*Distributed Ledger Technology*[3]): *A distributed record is a record that is shared, replicated and synchronized in a decentralized and distributed way.*

Docker: Virtual package management system (containers) that allow a more automatic and controlled installation.

Virtualized Environments: Technically speaking, it is the possibility of having machines (computers) running in a virtual way (not as a physical machine) within a physical machine or several.

***Core* Team:** People voluntarily assigned by the Associates performing support, development and research functions of new functionalities to be incorporated into the T Network platform.

Management Engine Team: People dependent on the General Directorate of Alastria with the function of energizing and promoting the collaboration of associates.

Bastion Guide: Instructions to carry out a securisation (provision of technical levels of security or assurance) of a computer installation.

GitHub: Version control system, widely used by the developer community and used by the Alastria Network Consortium Association to locate, reference and access open *software*

[2] Cf. NATIONAL INSTITUTE OF CYBERSECURITY (INCIBE), https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/bastionado-sistemas-y-servidores

[3] ITU (2019) "Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions": "Distributed Ledger is a type of ledger that is shared, replicated and synchronised in a distributed and decentralized manner"

created collaboratively by its Associates.

IBFT (*Istanbul Byzantine Fault Tolerance)*: Consensus mechanism established between the nodes of a *blockchain* network to make the decision whether or not to join a block to the blockchain, where an efficient tolerance of faults or non-compliances is pursued, that is, an algorithm that achieves consensus among a greater number of honest (fault tolerant) nodes than dishonest (non-compliant, fraudulent, failed or faulty nodes).[4 y 5]. Part of the BFT family of consensus mechanisms.

Permitting List: List of nodes that have been enabled in a *blockchain* network.

Consensus Mechanism[6]: Rules and procedures by which the nodes of a network determine and agree how to validate a set of transactions.

Permitting Mechanism: Function that enables or disables communication between the network nodes based on a series of manual or automatic rules, within a permitted public network scope.

Best Efforts: Civil liability standard for fault or negligence of node managers that requires them to monitor the activity of the node in accordance with the rules and policies of the network and to follow good professional practices and standards of operators (lex artis), in order to prevent any nodal damage to third parties.

Node: Computer or process that connects to a DLT network and uses the peer-to-peer protocol (P2P) that allows these machines to communicate with each other within the network, as well as disseminate information about transactions and blocks. According to ITU, it is "a process or device that participates in a DLT"[7]

Critical Nodes: In the T Network they are defined as those nodes without which the network cannot function, given the nature of the function they perform.

Permitting Nodes: They run the Quorum *bootnode* function[8] to allow node discovery on a peer

[4] ITU (2019), ITU-T Technical Specification FG DLT D3.1, *DLT Reference Architecture,* August, sub 6.1.5.3.

[5] Consensys Inc.(jun-2018) https://media.consensys.net/scaling-consensus-for-enterprise-explaining-the-ibft-algorithm-ba86182ea668

[6] ITU (2019) "Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions": "Consensus mechanisms are the rules and procedures by which consensus is reached" and "Consensus is an agreement that a set of transactions is valid"

[7] ITU (2019) "Technical Specification FG DLT D1.1 - Distributed ledger technology terms and definitions": "node is a device or process that participates in a distributed ledger network".

[8] Quorum is developed by JPMorgan and can be found at https://www.goquorum.com/

to peer network. Without acceptance by one of these nodes, a new node cannot join the network.

Regular Nodes: They participate by replicating the *blockchain*, accepting the blocks generated by the validators and executing the transactions included in them. They are also allowed to inject transactions into the Network from sources external to the *blockchain*.

Validating Nodes: Nodes that are in charge of guaranteeing the consensus of the network and the generation of blocks. To do this, they run the consensus algorithm (IBFT)[9].

Permitting: Authorization or enabling of the Permitting Nodes to the Regular Nodes so that, using the gas limit granted, they propose (initiate), carry out (write), or consult (read) transactions.

Quorum: *Software* from JPMorgan, a client of the Ethereum network that incorporates characteristics of a permitted *blockchain*, such as allowing private transactions and changing the way in which the inclusion of blocks in the *blockchain* chain is decided.

Public *Software* Repository: Centralized space where digital information is stored, organized, maintained and disseminated, usually computer files, which may contain scientific works, data sets or *software*.

Resilience: Ability of a system to recover from incidents that may occur.

RTO (*Recovery Time Objective)*: Desired time for a computer asset to recover following an incident.

RPO (*Recovery Point Objective*) - Target recovery point understood as the amount of data that can be assumed to be lost in the event of an incident following a system failure. Defined in time as it is the period that elapses between the moment of the disaster and the last point of data restoration in a backup copy.

Operating System: A piece of *software* that manages the hardware resources of a machine.

Solidity Command Line Interface (solc): Solidity is a programming language for *Smart Contracts* in *Ethereum*. *Solc* is a type of command line compiler with no graphic interface for that language.

Private transaction: Transaction only known by the sender and receiver.

[9] IBFT - Istanbul Byzantine Fault Tolerance

Validation: Process by which the Validating Nodes verify that the received transactions comply with the established IBFT protocol, ensure the formation of transaction blocks, the correspondence of cryptographic keys in the blockchain and, ultimately, the unit thereof.

VPN (*Virtual Private Network*): Telematic connection between two computers using cryptographic techniques that guarantee the privacy of communication between them.

Web3j: Highly modular, lightweight Java and Android library to work with *Smart Contracts* and integrate clients (nodes) over *Ethereum*-type networks[10].

[10] https://docs.web3j.io/

1. Introduction, Objectives and Scope

The Alastria Network Consortium (hereinafter ALASTRIA, the ASSOCIATION or the CONSORTIUM) is constituted as an association under Organic Law 1/2002, of March 22, regulator of the Law of Association. ALASTRIA has full operating capacity and has been registered in the First Section of the National Registry of Associations with number 616096.

ALASTRIA operates non-profit and its main objective is to create a community made up of all kinds of public and private organizations, as well as individual experts, to promote the implementation, standardization, protection and use of technologies such as Distributed Ledger Technologies (DLT), promoting knowledge and use by Spanish society of this technology, promoting its use among administrations, companies and other social agents.

ALASTRIA, as a non-profit community dedicated to promoting distributed networks and infrastructures (*blockchain*), under the principles of absence of commercial interest and technological neutrality, thanks to the collaboration of its associates (The Associates), has developed the infrastructure named T Network (the "Network" or the "Alastria Partner Network") in order that its associates can carry out concept/product/activity tests, under the conditions determined in each case.

Article 3 of the ALASTRIA statutes ("Purposes and activities") establishes that the Basic Technological and Operational Guides, under primary or principal documented form of Network Operation and Government Policies ("Government Policies"), will establish the protocols and *blockchain* standards that will be adopted by networks that follow the ALASTRIA standards (Technology Guide) and will be completed when necessary with technical sub-policies for permitted and node governance (critical or regular). At all times, priority will be given to criteria of technological neutrality (absence of preferences over a specific technology) and universality (attempt to enable the maximum number of technological protocols that allow the use and greatest possible adoption of the network).

The "**T Network" is a permitted public network**[11] accessible to any user with a computer and an Internet connection. The Regular Nodes that participate in it must be accepted by the Permitting Nodes, but the default transactions are public. This means that the Critical Nodes participate in the maintenance and security of the Network and that all transactions, unless they decide to use Private Transaction features, are visible to the different Nodes.

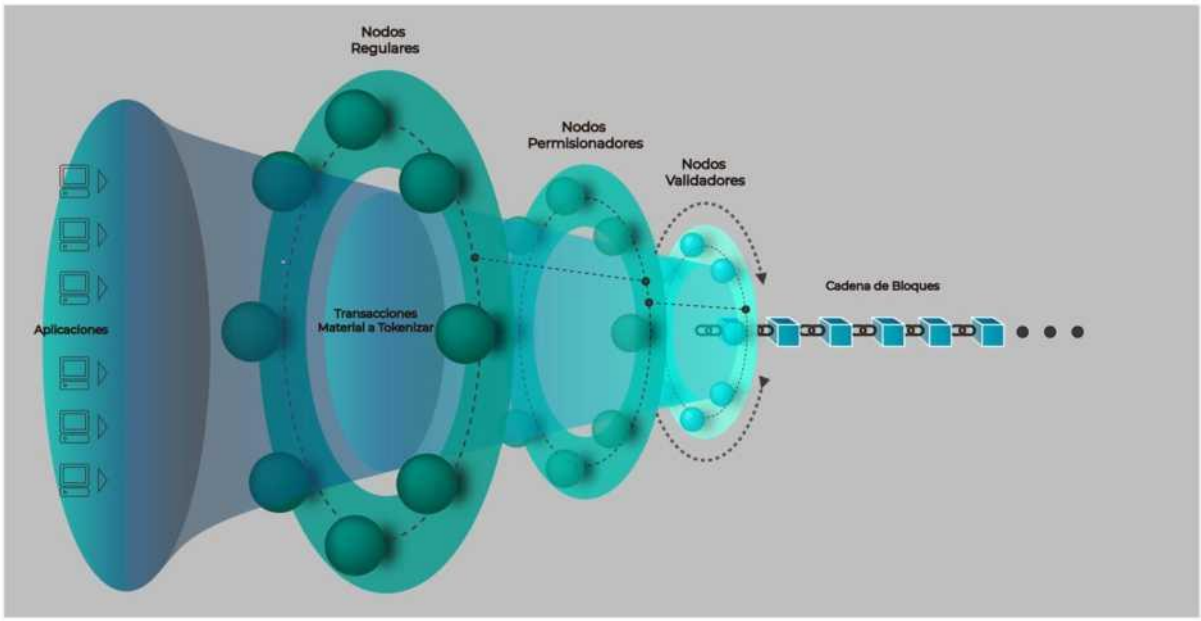
[11] According to the classification of the ITU(International Telecommunications Union): https://www.itu.int/en/ITU- T/focusgroups/dlt/Documents/d12.pdf Section 4 the T Network would be a permitted type of network

This document is written in compliance with the provisions of the statutes of the ASSOCIATION, taking into account the different types of node that exist and their role within the Network.

This document defines how the operational and governance elements are established in the T Network, including the Permitting Policy[12], it defines what must be taken into account when installing a Critical Node[13] and operating it by the Associate when installing it on the Network, what issues should be taken into account in the management of a Regular Node and, finally, the operation of the Critical Node Emergency Committee.

[12] See glossary for definition of "Permitting".
[13] See glossary for definition of Critical Node.

2. Description of the Architecture of the Alastria Partner Quorum[10] type Network (T Network)



In the Quorum Type network ("T Network") there are basically three types of nodes, depending on their role on the network:

Validator (block-maker)	The validating nodes execute the consensus algorithm, which in the case of this T Network is the IBFT.
Permitter (Bootnode)	Are nodes whose physical addresses ("enodes") are perfectly known throughout the network. The network nodes only know the bootnodes that they have in their permitting file. Through a bootnode, the nodes of the network cannot know more nodes.
Regular (general)	A node that participates by replicating the *blockchain*, accepting the blocks generated by the validators and executing the transactions included in them. They are also allowed to inject transactions into the Network from sources external to the blockchain.

The software required for all nodes[14], their installation and connection to the T Network of the Alastria partners is described in the GitHub[15] and Docker[16] tools that have been created in the ALASTRIA public *software* repository.

[14] The Intellectual Property Policy applicable to all the software of the T Network Nodes existing in the official repositories is referenced in Annex IV of the Alastria Official Statutes.

[15] https://github.com/alastria/alastria-node

[16] https://hub.docker.com/r/alastria/alastria-node-general.

2.1. Validating Node

The T Network **Validating Nodes**[17] execute the Quorum[18] IBFT consensus algorithm that makes the nodes go consecutively, performing the work of proposing the addition of a new block to be added to the chain. Given the criticality of these nodes in the proper functioning of the Network, it has been determined that the validating nodes **exclusively carry out the execution of the consensus algorithm** and do not allow its use for other functions. Specifically, the Associate that operates a Validator Node, will not be able to use it to deploy contracts, initiate transactions or perform blockchain chain reading operations: they will only be able to use it to execute the consensus algorithm.

In other words, Validator Nodes must not have any type of connectivity with business systems, run software other than that of the validator node, or share resources with other corporate functions. The software[19] that is executed by the Validating Nodes is the one specified[20] and recommended by these technical policies. The Validating Nodes undertake not to alter or modify the recommended software without the knowledge of the Association's technical team and the other critical node operator Associates. Any modification of the indicated software will be made under the exclusive responsibility of the critical node manager, without in any case being able to compromise the operation or security of the Network.

Validating Nodes can only be connected to other Validating Nodes and one or more Permitting Nodes. In other words, the Validating Nodes will be configured so that they do not accept connections from any regular node, via the Quorum permitting mechanism. In this way, the number of connections of a Validator Node with other Nodes is limited, independent of the size of the network and, in this way, the technical requirements can be managed for the execution of the consensus algorithm as well as the security measures to implement in the Node.

2.2. Permitting Node

A **Permitting Node is a node that executes the Quorum[21] bootnode function**, but which also has other functions and restrictions in terms of connectivity with other Nodes on the Network.

The Permitting List of each one of the Permitting Nodes will contain, in addition to the

[17] In this document, we will use the term "validator", but it is equivalent to "block-maker" or "builder" or "miner" in other references.

[18] Quorum is developed by JPMorgan and can be found at https://www.goquorum.com/

[19] The Intellectual Property Policy applicable to all the software of the Alastria Nodes existing in the official repositories is referenced in Annex IV of the Alastria Official Statutes.

[20] The official repository is at https://github.com/alastria/alastria-node.

[21] Quorum is developed by JPMorgan and can be found at https://www.goquorum.com/

Validating Nodes, the list of the Regular Nodes that have been accepted in the Network.

In this way, the Permitting Nodes will **connect on the one hand with the Validating Nodes and on the other with the Regular Nodes**, isolating the validating nodes from the permitting management and from the connections with the regular nodes.

The physical addresses of the Permitting Nodes (similar in concept to Internet IP addresses) will be public and well known, so that the Regular Nodes can initially connect to the Network.

The benefits obtained with this configuration are the following:

- The resources necessary for Network connectivity of the Validating Nodes are kept constant, being able to dedicate all the resources of the machines to the execution of the IBFT consensus algorithm, regardless of the number of Regular Nodes of the network.
- The configuration changes of the Validating Nodes are reduced to the minimum necessary, and are always related to the execution of the consensus algorithm. Specifically, it is not necessary to update the permitting list in these nodes, even if the Regular Nodes change. A reduction of the necessary changes in the Validator Nodes results in greater stability of these nodes. An update to the permitting file may be required in the event that a new validator is added to the IBFT consensus which has been allowed later than the last update of the permitting file.
- By reducing the exposure of the Validating Nodes to the rest of the Network, the technical implementation of the security and bastion policies of the Validating Nodes described in the corresponding section of this document is more efficient.

2.3. Regular Node

Regular Nodes[22] are those that allow Associates to participate in the Network, deploying contracts, initiating transactions, executing Smart Contracts[23] and performing blockchain reading operations.

The Regular Nodes are connected to the business systems of the entities that operate them (Associates) and have no greater technical restrictions than those of the internal policies of each of the entities that own and manage them, associated with ALASTRIA.

[22] In this document we will use the term "regular" to refer to this type of node. In other documents it is named “general”.

[23] Smart Contract - Technical Specification FG DLT D1.1Distributed ledger technology terms and definitions, definition 6.51, and section A.7.

3. Permitting Policy

3.1. Preliminary Considerations

According to standardization criteria, the **T Network is classified as a Permitting[24]/Public network**, in contrast to Public/Non-Permitting networks (Bitcoin[25], Ethereum[26]), and also different to private networks.

However, in other areas, other classifications are used that use similar, but not identical, criteria, which may generate some misunderstanding in the discussion about certain not yet fully defined characteristics of this type of network and that may influence the inclusivity and the policies of use of networks such as the T Network. In fact, the exact model of the Permitting implemented in the Network has implications in the Sovereign Digital Identity[27] (ID_Alastria) model, which needs to provide natural person access to the blockchain, either directly or indirectly.

To clarify concepts, some of the most important characteristics and implications of Permitting are set out below.

3.1.1. Permitting of all nodes or of only some nodes

In some areas, a distinction is made between permitting networks and public networks, a distinction based on whether permitting is required for all nodes in the network or only some of them.

It may be considered that, if all nodes are required to be permitted, regardless of whether their activity is write or read, then they are private networks.

[24] That is, it "requires authorization to carry out one or several activities" on the network (sic, ITU (2019), ITU-T Technical Specification, FG DLT D1.1, Distributed ledger technology terms and definitions, 1 August 2019, sub 6.42. In accordance with these standards Alastria is a "permissioned DLT system" (ITU, ibid., sub. 6.41) where "permits are required to maintain and operate a node"; being public as well (ibid., 6.49) and therefore "accessible for public use".

[25] Bitcoin https://bitcon.org/.

[26] Ethereum https://www.ethereum.org/.

[27] Self-Sovereign Identity (Digital). In Technical Report FG DLT D1.3 (DLT Landscape Standardization a reference may be found to DID de ID_Alastria.

Similarly, it can be considered that a public-allowed network is one that requires the permitting of a subset of the nodes (for example, the nodes that have write capability), not requiring the permitting of other nodes (for example, the nodes that only have read access).

3.1.2. Network *Inclusivity*

With this last approach, a network of these characteristics requires permitting only for the nodes that can modify the blockchain, while the status is completely public and anyone can access in read mode and, therefore, audit the Network. This point of free reading access does NOT occur in the case of the Alastria Partner Node T Network as specified below.

3.1.3. Implementation Considerations

From a technical point of view, **with Quorum technology derived from Ethereum, it is not easy to implement a Permitting limited to Nodes that modify the status of the blockchain.** Currently, **in Quorum the Permitting is at node level and is all-or-nothing**, that is, a node that participates in the network no longer has any read/write limitations, as long as the actor using that node has an account with enough gas to start transactions.

Quorum's current permitting mechanism implies that **all nodes have to be permitted even if they only query**, since they must replicate the *blockchain* on their disk.

In this situation, an actor who wants to query and who does not have a permitted node should access the network through the node of some other entity that does have an already permitted node. It would then be the responsibility of the latter entity to control transactional activity in the network of the *"delegated"* entity.

This already occurs in completely private networks, where the entities participating in the *blockchain* provide activities to their clients (individuals or companies) without requiring them to have nodes in the network. Although in most cases, the client entity never has direct access to the *blockchain*, and all transactions are initiated and signed by the entity that operates or manages the node.

3.1.4. Alastria permitting model

Returning to the classification developed in various standardization bodies (UNE, W3C, ISO ...), such as, for example, ITU-T FGDLT, the T Network can be defined as a public-licensed network. ALASTRIA chooses to require that all nodes be permitted[28].

[28] V. supra, note 21.

The implications derived from this consideration are as follows:

1. There can be no "anonymous" nodes that allow anonymous actors access in write and read.
2. If an entity allows *blockchain* access (both read and write) to other entities through the node that operates on the Network, it (the entity that operates the node) is responsible for all the actions that are carried out through its node in the *blockchain*, with the implications that derive from it.

With the current version of Quorum, the permitting is at node level and not at entity level. In other words, **an entity can have more than one node, it being necessary to permit each one independently**. It is already planned to evolve in the future to a more sophisticated permitting system, based on Smart Contracts that automate the current model and that allow permitting to be managed more efficiently.

The current permitting process in the T Network consists of two manual parts that will evolve towards automatic processes based on Smart Contracts: a first technical part and a second administrative part. With the first, the technical part, the Associate must make a request through GitHub, formalizing a file[29] update request to incorporate the Node data into the Node declaration files. These files are located under the *alastria/alastria-node* repository and are the following three files:

- DIRECTORY REGULAR.md
- data/regular-nodes.json
- data/constellation-nodes.json (This file is only necessary if we have activated Constellation, Quorum's private transaction mechanism in our node).

Once the Associate makes this request in the GitHub tool, the *Core* Team automatically receives a notice to carry out a technical verification in which it will be verified that the files have been correctly modified, that the Node is displayed correctly and is properly installed.

In addition a request must be made via form https://portal.r2docuo.com/alastria/forms/noderequest where a formal permitting is requested from the Association. If this is all correct at a technical level, this second administrative review is carried out to verify that the Associate meets the prerequisites required (being a member of ALASTRIA without any type of administrative or legal problem that prevents the node from being incorporated). If everything is correct, the Core Team proceeds to incorporate the file changes to the system and the Node ends up being visible to the Network as soon as one of the Permitting Nodes (*bootnode*) updates the configuration files.

[29] This update request is called "Pull Request" on GitHub.

In the coming months, it is planned to automate this functionality using Smart Contracts[30], in order to allow decentralized management of the Permitting function, based on a request for credentials from the Nodes requesting its inclusion and automatic authorization from the Network. The criteria that are established to carry out this automation, once approved, will be reflected in a new version of this document.

3.1.5. Network De-Permitting Model

It may be necessary to de-permit, disable, disallow, revoke or terminate the validity of the authorization or permission of the Node that has been included in the T Network. The causes may be voluntary or involuntary. The first ones take effect at the request of the managing Associate of the node in question (for example, the Associate withdraws from the ASSOCIATION) and the second ones take effect at the request of the ASSOCIATION itself (due to the breach of the obligations inherent in the condition of Associate managing the Node, either at an administrative level (such as non-payment of a fee) or at a technical level (such as inappropriate use of the Network or for non-compliance with the rules and policies of use of the Network. In these cases, the Core Team will proceed to modify the three files indicated above, eliminating the references to the node that has been requested to de-permit, and finally, the *bootnodes* will be restarted after updating their configuration files.

In the event that an Associate wants to de-permit a node, it must notify it at least 15 business days before the date of its effectiveness.

When the automatic management of the Permitting and De-Permitting based on *Smart Contracts* is developed, this process will be automated, fulfilling the objective of maximum decentralization of the Network administration. As mentioned previously, the criteria that are established to carry out this automation, once approved, will be reflected in a new version of this document.

4. Technical Operation Policies and Recommendations linked to the Permitting

4.1. Technical operating policy for Permitting Nodes

Associates must comply with the following "Permitting Policy":

- **Any Node that wants to have access to the Network must be permitted** in the T Network (by technical design) although in future types of networks it may be possible to allow read-only access to non-permitted nodes as in other networks (eg. LacChain).

[30] Smart contract consisting of a "program written in the distributed registration system that encodes the rules for specific types of transactions in a way that can be validated and executed under specific conditions" (ITU (2019), FG DLT D1.1, sub 6.51.

- The permitting request is made through the GitHub tool through a Pull Request and an online form. This request is evaluated, at a technical level, by the *Core* Support Team of the platform and, at an administrative level, by the Management Engine team, after which the authorization or denial of use of the network is made. These requests are registered in the version control existing in said tool.
- The critical function of Permitting Nodes is to not allow unilateral connection of unidentified and authorized nodes in the official list maintained by ALASTRIA.
- Permitting Nodes must be protected from external connections by Bastion standards[31].
- The Associates that manage Permitting Nodes **must necessarily comply with the Conditions established in the Document "T Network Operating Conditions by Critical Nodes"[32]**.
- It is recommended to use the software versions of the existing Permitting Node specified in the official ALASTRIA repository and keep nodes updated with the latest versions.
- For security reasons, other processes should not be executed on the same machine where the Permitting Node *software* is running, the machine being understood as the virtual part of a physical machine, if any, so that the use of said machine space is absolutely compartmentalized between the Node and other processes of the Managing Associate of the Validator Node.
- It is recommended not to modify in a particular way the *software* of the Validator Node, accepting it in all its terms and without the purpose of changes with the commitment to assume updates in all its terms. As the case may be, the modification must be carried out using the mechanisms established through the Pull Request on GitHub.
- Prior to the inclusion request of the Validator Node, ensure that the "*netstats*"[33] network visualization tool sees the new node and that its activity is properly reflected.
- In case the Associate operator of the Validator Node wants to unsubscribe their node from the permitting function, they must communicate it by the established procedure of Pull Request in GitHub at least 15 working days in advance that allow evaluating if it is necessary to activate any contingency plan in light of possible Network unavailability.

[31] Bastion means the instructions and technical actions that must be taken for the physical and logical protection of node security.

[32] https://portal.r2docuo.com/alastria/document?L62DE71FFF

[33] https://netstats.telsius.alastria.io/

•

5. Technical Operation Policies and Recommendations for Critical Nodes (Validators or Permitters)

5.1. Resilience Requirements

Resilience requirements apply mainly to Critical Nodes, due to their criticality and importance in the proper functioning of the Network.

5.2. Physical Security of Critical Nodes[34]

The Validating Nodes **exclusively perform the execution of the consensus algorithm**, its use for other functions being prohibited. This exclusivity applies to the portion of the machine where the *software* of the node in question is running, and it must be perfectly compartmentalized.

Critical Nodes must not have any type of connectivity with business systems nor run *software* other than that of the Critical Node or share resources with other corporate functions of the Associate. The *software* recommended for use by the critical nodes is that specified by these ALASTRIA Technical Policies.

Given their technical characteristics, the Critical Nodes must be housed in Virtualized Environments, either within the physical systems of the Associate operator of the node in question (CPDs[35]), or in systems located in the Cloud and managed solely by the Associate.

Depending on the location, certain additional considerations regarding the security of the Critical Node must be taken to guarantee its physical integrity, as well as establishing a monitoring access control and a sufficient isolation system to avoid its unwanted manipulation:

- **Critical Nodes located in CPD:** the CPD itself must have restricted access, that is, it must be located in a controlled and monitored area either within the Associate's facilities or offices or subcontracting the service provided it meets the following security and transparency conditions with ALASTRIA, with some type of centralized and automated access control system that also has a list of users and/or administrators authorized to access the CPD.

  Monitoring should record access to the CPD, as well as unauthorized access attempts. In addition, the records must be accessible to the personnel accredited by ALASTRIA for

[34] Work is underway to ensure full alignment with ISO standard 27001.
[35] Data Processing Centre.

the performance of the necessary audit tasks.

On the other hand, the physical access itself to the platform (server) that runs the Operating System (virtualized or not) must in turn be limited, its access must be isolated and, more so, restricted to the administrative personnel in charge of the administration, support and maintenance activities of the Critical Node in the Network.

It is recommended that the platform where the Critical Node is housed is physically separated from the Associate's other IT systems or, at least, is dedicated exclusively to covering the activity of the Critical Node installed on the Network, in order to prevent its accidental or intentional manipulation by personnel outside the activities of administration, support and maintenance of the Critical Node.

- **Critical Nodes located in the Cloud:** The Critical Nodes that are located in the Cloud of any of the service providers (AWS, Google, MS ...), even though they are physically located within the physical facilities (CPD) of a third party, must also have physical security measures that guarantee restricted access, access monitoring and sufficient isolation to avoid undesirable manipulations of the Critical Node.

  To ensure that the Critical Node has sufficient physical security measures, it will be necessary for the indicated service providers to also have security policies that guarantee the physical protection of the critical node in the same way as for the critical nodes located in a CPD in the facilities or offices of the Associate owner and operator of the Critical Node.

  In addition, each Associate Critical Node operator in the Network shall periodically monitor, verify that the providers' physical access security policies are up-to-date, that the controls that the providers perform on their physical systems are sufficient to ensure appetite of risk for the Critical Nodes, and that the audits and certifications of compliance are carried out satisfactorily. In this way, correct management of the physical security of the CPDs of the cloud service providers can be verified.

5.3. Bastion

Given the type of operating system executed by the Critical Nodes (64-bit Linux), the Bastion of these systems must be carried out following the Bastion Guide. It is mandatory to use Ubuntu 16.04[36], and it is highly recommended to use *Red Hat* as the operating system in Critical Nodes[37].

The following checklist[38] includes the main aspects to take into account in a Bastion (mainly in-house) based on RedHat but can be easily adapted to:

	Action	CIS
	Physical Security and Preparation	
1	If the equipment is a new installation, it must be protected from hostile network traffic until the operating system is installed and bastioned.	
2	Set a password for BIOS/firmware.	
3	Configure the boot order of the devices to prevent booting from external devices.	
4	Use the latest possible version of RHEL (if RedHat is used as the Operating System) or use the latest version of Ubuntu Software, CentOs, etc. bearing in mind that the installation scripts created have been considered for Ubuntu 16.04	1.7
	File System Configuration	
5	Create a separate partition with nodev, nosuid, and noexec options set to /tmp.	1.1.1-.4
6	Create separate partitions for /var, /var/log, /var/log/audit and /home.	1.1.{5,7,8,9}
7	Link the assembly from /var/tmp to /tmp.	1.1.6
8	Set the nodev option to /home.	1.1.10
9	Set the nodev, nosuid, and noexec options to /dev/shm.	1.1.14-.16
10	Set the "sticky bit" option on all writeable directories.	1.1.17
	System Update	
	Register the system on Red Hat Satellite Server in order to receive	
11	updates and patches or activate automatic updates in the different operating systems other than RedHat	1.2.1
12	Install the Red Hat GPG key and enable the gpgcheck service when using Red Hat	1.2.2-.3
	Secure Boot Configuration	
13	Set root as owner of user/group and give read and write permissions only to Root in /boot/grub2/grub.cfg	1.5.1-.2

[36] Resilience Commission Decision of 19Feb2019.

[37] In case of choosing Red Hat it is important to note that the automatic installation procedure existing in the alastria-node/alastria repository is not valid and it will be necessary to install the node manually.

[38] This checklist has been provided by the Resilience Commission in 2018.

14	Set the boot loader passwords.	1.5.3
15	Delete the X Window system.	3.2
16	Disable the X Font server.	
	Process Bastion	
17	Restrict core dumps.	1.6.1
18	Enable the Randomized Virtual Memory Region Placement.	1.6.2
	Operating System Bastion	
19	Delete legacy services (e.g., telnet-server; rsh, rlogin, rcp; ypserv, ypbind; tftp, tftp-server; talk, talk-server)	
20	Disable any service launched by xinetd o inetd that will not be used.	
21	Delete xinetd, if possible. Delete other legacy services (e.g., chargen-dgram, chargen-	2.1.11
22	stream, daytime-dgram, daytime-stream, echo-dgram, echo- stream, tcpmux-server)	2.1.{12-18}
23	Disable default services that will not be used (e.g., FTP, DNS, LDAP, SMB, DHCP, NFS, SNMP, etc.)	
24	Enable Daemon umask	3.1
	Firewall and Network Security Configuration	
25	Limit connections to enabled services to those authorized users using firewalls or other access control technologies.	4.7
26	Disable the IP forwarding.	4.1.1
27	Disable sending of redirect packets.	4.1.2
28	Disable packet acceptance with redirect path set at source.	4.2.1
29	Disable acceptance of ICMP redirect packets.	4.2.2
30	Ignore Broadcast request packets.	4.2.5
31	Enable protection against Bad error messages.	4.2.6
32	Enable TCP/SYN cookies.	4.2.8
	Remote management using SSH	
33	Set protocol SSH to 2.	6.2.1
34	Set log level from SSH to INFO.	6.2.2
35	Disable Root login for SSH.	6.2.8
36	Set SSH PermitEmptyPasswords to No.	6.2.9
	System integrity and intrusion detection	
37	Install and configure AIDE.	1.3.1-.2
38	Configure SELinux.	1.4.1-.6
39	Install and configure OSSec HIDS.	
	Event registration	
40	Configure Network Time Protocol (NTP). Set the Spanish time zone (GMT +1) based on the server hora.roa.es	3.6
41	Enable system audit (auditd).	5.2
42	Install and configure rsyslog.	5.1.1-.4
43	All root accesses must be audited.	

44	Configure the sending of logs to an external system (e.g. Splunk).	5.1.5
	Access to files and directories	
45	Enable and test integrity checks on system accounts, group membership, and associated permissions.	
	PAM Configuration	
46	Ensure that the configuration files of PAM, /etc/pam.d/* are safe.	6.3
47	Set the password hashing algorithm to SHA-512.	6.3.1
48	Set robustness measures in the creation of passwords.	6.3.2
49	Restrict root access to the system console only.	6.4
	Warning Panels	
50	Set a warning banner on physical accesses to the system console.	6.2.14, 8.1
51	Set a warning banner on remote accesses to the system console.	8.3
	Antivirus Considerations	
52	Install and enable an Anti-Virus software.	
53	Configure the daily update of Anti-Virus signatures.	

5.4. Integrity

The integrity and maintenance or continuity of the functionality of the Critical Node must be protected and ensured taking into account the following points:

- **Minimum number of Critical Nodes active in the network:** in order for the T Network to operate correctly, guaranteeing optimal and safe activity, it is necessary that at least **5 Validating and 2 Permitting Nodes be active.**

- **Optimal number of Critical Nodes active in the Network:** in the Network, the optimal number of Critical Nodes would be twenty-one (21) Validating Nodes active, 6 Validating Nodes in stand-by and 8 Permitting Nodes.

- ***Software* compatibility and versioning:** the software that runs on the Critical Nodes, both the T Network's own software and the rest of the software that the Network uses or is necessary for the safe and correct operation of the node in question **must be updated to the latest version**[39]. Updates must use software repositories certified by their own developers, following the respective integrity controls (HASH verification, digital certificates, etc.).

- **Critical Node Monitoring:** The operation of the Critical Node, as well as the state of its integrity and security, must be continuously monitored and **under the**

[39] The latest version of the software available to Alastria partners is at https://github.com/alastria/ and is installed by each partner at their own risk and expense.

control of a dedicated management team that has been notified to the Association. Local access to Critical Nodes must be enabled at the Operating System level, as well as with software for security and/or remote management.

- **Inclusion and forfeiture of nodes:** The registration and withdrawal of the Critical Nodes will be required to be **notified by the Associate two (2) weeks in advance and validated by personnel accredited by the CONSORTIUM.** The activities of inclusion or forfeiture of the Critical Nodes must be planned, controlled and tested at the end, in maintenance windows that guarantee that the Network is not affected. Said activities must be documented, registering any type of incident, following the protocols and pertinent reversing actions in case of failure or serious incident that may affect the rest of the Network.
- **Network orderly stop (network shutdown):** When for organizational or force majeure reasons, it is decided that the Network should be stopped (turned off), the Associate managers of Nodes in said Network will be notified, requesting their approval by means of a signed note, indicating the procedure to follow to save a copy of the existing blockchain that can be saved as a backup.

5.5. Availability

To guarantee optimal levels of availability of the Network and its correct operation, it will be necessary for the Critical Nodes to have the corresponding monitoring systems of each Associate enabled, as well as the effective backup mechanisms and recovery procedures.

- **Monitoring:** as detailed in the previous section, in addition to monitoring the integrity and security of the Node, it must have monitoring mechanisms that allow it to verify its correct operation, both at the Operating System and hardware level as well as the software level of the Network.

  The software must execute its monitoring protocol, verifying that the monitoring port (TCP 8443) is open and available to the T Network For additional protection, this port must be restricted to one or more IPs that will be established by the Critical Node Committee, and that will be held by the Core Team.

  In addition, there must be a network alert and monitoring mechanism in case of denial of service (DoS[40]) attacks that may affect the availability of the activity or the access of the Critical Node to T Network.

- **Backup:** Although the need for a traditional backup of Critical Nodes is not necessary

[40] Denial of Service.

per se given that blockchain data is de facto backed up in each and every other Network Node, it is recommended that each Associate manager of a Node has some type of backup mechanism for it both in the software and in the data (backup, snapshot[41], etc.) that guarantees the total recovery of the information necessary for the reactivation of the Critical Node, within the maximum time of unavailability, after a failure or damage (intentional or accidental) thereof, thereby ensuring that important information or data is not lost. The above is especially critical to ensure that it is not necessary to sync the blockchain from the start.

The management of the backup mechanisms is the responsibility of the Associate operator of the Node in question, if the Node is hosted within its CPD. If it is hosted in a virtualized system in the Cloud, the Node operator Associate is responsible for verifying that the provider has the necessary backup options to cover the availability needs of the Critical Node.

- **Recovery times:** the Associate operator of the Critical Node must have a well-defined recovery plan and RTO/RPO recovery times, so that in a failure that affects one of the Validating Nodes, it is possible to recover and reactivate 100% the operation of said node within the defined times, affecting the operation of the Network as little as possible. This time will depend on whether the recovering node is the only one with the failure and does not affect the Network, or whether it is the Node that can cause the Network to fail as a whole.

  The referred recovery plan shall have detailed technical procedures aimed at achieving the recovery and reactivation of the affected Critical Node, as well as the definition of the responsibilities of the Associate personnel in charge of carrying out the recovery tasks.

5.6. Privacy

In order for the Critical Nodes to have the level of privacy necessary to comply with privacy policies and the treatment of sensitive information, maintaining the correct operation of the network[42], it will be necessary to have the following:

- **Internet Connection:** with a public IP that allows the visibility of the Network and all its Nodes, verifying that the Critical Nodes execute the functionalities that correspond to them in the ports dedicated to it according to technical requirements. Given that the visibility of the Node in question will be on the public internet, the necessary precautions should be taken, using the methodologies, mechanisms and technologies

[41] Copy (image) of the node's software at a specific moment in time.

[42] The use of the Network must be respectful of the General Data Protection Regulation and other applicable rules on the matter that are in force.

necessary to avoid enumeration of IP services, processes or other sensitive information different from that necessary for its connection to the T Network.

- **Data encryption:** Both the data in transit and the data stored in the Critical Nodes must be encrypted using strong encryption algorithms that do not present known vulnerabilities and that are compatible with the technologies and software necessary to execute the activities related to the T Network without affecting the performance of it.

  Data in transit includes the T Network's own data traffic, the traffic generated by communications from management, security or backup software running on the Node and communications from remote accesses from internal networks (Associate networks) or public networks (Internet or third parties).

- **Remote communication:** in case it is necessary to make connections from remote networks or equipment to the Validator Node for the exchange of data with sensitive information, monitoring of system data, remote control and access, etc., a VPN virtual private network connection must be used between the Validator Node and the remote system or network.

  The VPN must be managed and maintained by personnel accredited by the Node's Operating Associate, having a rigorous control of users who can access it through lists of users, administrators and allowed systems, and effective access control that uses said list of users.

5.7. Organisational requirements

It will be necessary for the Associate that manages or operates a Critical Node in its facilities to comply with an independent certification process with which the compliance of each of the elements exposed in that document is verified and that it can be contributed to the other members of the Consortium.

In the event that the Associate has a valid SAS70, ISAE3402 or SSAE16 certificate, or is classified as a critical infrastructure according to Law 8/2011, it will be exempt from complying with the independent certification process, provided that it accredits the ASSOCIATION compliance with the provisions of this paragraph.

6. Technical Operation Policies and Recommendations for Regular Nodes

6.1. Technical operating policy for Regular Nodes

The Associate manager of a Regular Node must comply with the following "Technical Policy for Regular Nodes":

- Not permit connection to other unauthorized Nodes in the official list maintained by the ASSOCIATION.
- Permanently update a list of elements permitted connection to the Node from external element accesses, in a file named "whitelist" located within the *Alastria Open Access*[43] component and that allows maintaining the general security of the Network.
- Use the versions specified in the official[44] repository and keep their corresponding Regular Nodes updated.
- Perform the installation of the Node under the specified installation directory.
- Not modify the software of the Network's Node. In case a modification is needed, this should be done using the methods established in GitHub[45].
- Ensure that the "*netstats*"[46] Network visualization tool adequately visualizes its Node and that its activity is adequately reflected, enabling the necessary IP[47] ports in the access network to provide said information on usage statistics.
- Limit the load on the Network within the limits established at all times within the technical policy in force, initially set at 25,000 transactions per day. And in case it is necessary to exceed this limit, request and obtain authorization from the Core Team.
- The Associates that manage Regular Nodes **must necessarily comply with the conditions established in the Document of Operating Conditions of the Network by Regular Nodes**"[48].
- Immediately communicate to the Alastria technical team and the Critical Node Emergency Committee[49]- the possible vulnerabilities that may be found on the Network and, where appropriate, not exploit them for their own benefit.

It is further recommended that the "Monitor"[50] component be activated, protected by firewall and accessible only from a specific IP managed by the Core Team and that, activated by the Critical Node Emergency Committee, serves to allow emergency actions, such as a restart of

[43] https://github.com/alastria/alastria-access-point
[44] https://github.com/alastria/alastria-node
[45] https://github.com
[46] https://netstats.telsius.alastria.io/
[47] Necessary ports are described at https://github.com/alastria/alastria-node/README.md
[48] This document of Operating Conditions of the Network by Regular Nodes is available at https://portal.r2docuo.com/alastria/document?LAA4CC6A0B
[50] This component can be installed from https://github.com/alastria/monitor or in the standard node installation process by answering "S" to the corresponding question.

the node in case of malfunction and no attention from the Associate managing it.

7. Critical Node Emergency Committee

7.1. Objective

The objective of this Committee as a part of incident management is to act as a line of defence, as requested by the Resilience Commission in case of malfunction or attacks on the Network.

7.2. Constituents

A designated person in charge of each of the Associates who have installed a Critical Node in the Network, a member of the Alastria Board of Directors and a member of the Management Engine team appointed by the General Directorate of Alastria will be part of it.

7.3. Function

The Committee will meet in person or remotely when called at the request of any of its members. Its main function is to evaluate a possible threat to the operation of the Network, either by malfunctioning of the Critical Nodes or by detection of an attack against the Network.

Among its possible actions may be performing a remote intervention on a Critical Node of the Network (through the Monitor tool) to execute a restart or shutdown of a Node or requesting an urgent de-permitting of a Node.

8. Network Use and Operating Conditions by Critical and Regular Nodes

8.1. Network Operating Conditions by Critical Nodes

Document by virtue of which the ASSOCIATE expressly declares to be aware of and undertakes to comply with all the internal regulations of the ASSOCIATION (Statutes, its annexes, government policies, codes of conduct, technical specifications and other operating agreements between their members and the ASSOCIATION) and to deploy its best efforts in accordance with professional standards, for the operation and maintenance of a Critical Node (either permitting or validating).

This document constitutes a commitment to the ASSOCIATION and to the other Associates.

8.2. Network Conditions of Use by Regular Nodes

Document by virtue of which the ASSOCIATE expressly declares to be aware of and undertakes to comply with all the internal regulations of the ASSOCIATION (Statutes, its annexes, government policies, codes of conduct, technical specifications and other operating agreements between their members and the ASSOCIATION) and to deploy its best efforts in accordance with professional standards, for the operation and maintenance of a Regular Node.

This document constitutes a document of good use of the network for the other Associates.