



Co-funded by
the European Union



Means of verification - M13

Recommendations for the further development of the EBSI eco-system

23.10.2024.



Disclaimer:

the content of the report not representative of the EU commission

| | |
|----------------------|--|
| Project title | EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE NODE EXPANSION (EBSI-NE) |
| Grant Agreement No. | 101102570 — EBSI-NE — DIGITAL-2022-DEPLOY-02 |
| Deliverable title | Recommendations for the further development of the EBSI eco-system |
| Version | 1 |
| Date | 21/10/2024 |
| Responsible Partner | SGAD |
| Authors | SGAD, SKS, NASK, LOGALTY |
| Contributing Partner | SGAD, SKS, NASK, LOGALTY |
| Reviewers | SGAD |
| Dissemination Level | PUBLIC |

Recommendations for the further development of the EBSI eco-system

- 1. Infrastructure maintenance over the next 4 to 5 years:** National Competence centers (hereinafter NCCs) will be formed along with the organisational structure that will cater for the European Digital Infrastructure Consortium (hereinafter EDIC). NCCs will provide first-line support and organise knowledge sharing between Node Operators (hereinafter NOs). It is envisioned that there should be a NO community formed that could be a formal voice in EDIC decisions when technical, configuration, security, etc. issues arise. Financial aspects will be tackled as well, to have a sustainable ecosystem. Commercial services should be created as soon as possible, to cover infrastructure, NCC maintenance and personnel costs. EDIC could become a Network-as-a-Service provider for the specific industry use cases. Along with the commercial income, Member states could decide to provide financial contribution to the local Node operators to maintain network and NCCs using budget, funds, etc.
- 2. Integrating node operators into the EDIC structure:** Depending on the organisational structure of EDIC, node operators could form an organisational unit with an elected leader who could participate in the EDIC decision-making or explain new requirements to the community. This would allow more organised onboarding of a new NO, information distribution and control over the community. Moreover, Node operators will get the possibility to express their ideas or concerns to the community, and if needed, could be escalated to the EDIC management. As EBSI-NE project is aiming to create National competence centres formed from the Node operators mainly, EDIC will need to incorporate created organisational structure and NCCs as part of their support service.
- 3. Determining the provider of the electronic ledger service:** EDIC vs validator nodes: Electronic ledger service providers, regardless of qualified or non-qualified, should be organisations that govern the organisational structure of the electronic ledger. Thus, despite the distributed nature of Distributed Ledger Technology (hereinafter DLT), EDIC should become a formal electronic ledger service provider where validator nodes, hosted by the endorsed operators, would ensure not only technical reliability but legal certainty as well.
- 4. Identifying and developing measures for procedural and administrative checks needed to provide the electronic ledger service:** A common requirement for non-qualified and qualified trust service consists in identifying and developing appropriate measures for registration and onboarding procedures related to the trust service subjects, i.e., the natural or legal persons using the electronic ledger service, according to the portfolio. Typically, these users will be

sending transactions for execution in the infrastructure and, therefore, must be identified and properly authorised, as EBSI is a public permissioned ledger service.

5. **Cataloguing legal requirements of the electronic ledger service, including eIDAS 2, DSA, NIS2, etc:** Offering electronic ledger services to the public is regulated under the Electronic Identification, Authentication, and Trust Services 2.0¹. (hereinafter eIDAS 2 Regulation), which defines the electronic ledger as a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records. The eIDAS 2 Regulation allows both centralised and distributed ledgers, both of which can be non-qualified and qualified. The eIDAS 2 Regulation impose legal requirements to the provider or providers that record electronic data in an electronic ledger. There are more requirements if the ledger is to be qualified. Other regulations apply to this activity, such as Network and Information Systems Directive² (hereinafter NIS2), which considers trust services as essential services, or the Digital Services Act ³(hereinafter DSA), especially the liability regime for contents recorded on a ledger using smart contracts. Having a full catalogue of the legal requirements for the service is therefore of the utmost importance.
6. **Defining policy and security requirements for non-qualified and qualified electronic ledgers and alignment with the ISO/IEC 27002 ⁴control set:** All trust services typically are subject to a set of well-defined policy and security requirements, based in ETSI EN 319 401, a subset of ISO/IEC 27002 controls selected and tailored for all trust services. Other additional policy and security requirements are specific for each trust service, according to the result of a risk assessment and the application of the required measures to ensure the quality of the services, i.e. the ledger. This will include node management, ledger management, cryptographic controls, and others. The results of this work will feed the proposed CEN/CLC/JTC19 Technical Specification, to be referenced in the future Implementing Act.
7. **Identifying and developing measures for registration and onboarding procedures to the electronic ledger service:** The electronic ledger service, as other trust services, is subject to a minimum set of procedural and administrative controls, which need to be identified and properly developed, both in the case of qualified and non-qualified ledgers. These are additional to any controls that are required under NIS2, and may typically include policies and practices, terms

¹ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401183

² [EUR-Lex - 02022L2555-20221227 - EN - EUR-Lex](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1729605438388)

³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1729605438388>

⁴ [ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls](https://www.iso.org/standard/72431.html)



and conditions, agreements, management controls, business continuity or termination plans.

8. **Completing and detailing relevant measures for the management and implementation of the electronic ledger service:** The relevant measures for the maintenance and implementation of the electronic ledger service could be part of the EDIC - NCC common ground internal procedures that can be better defined once the centers are "activated". The EDIC on the direction and NCC as backing force behind the technical ones.



Funded by
the European Union