

DSCI Feedback on the Building Trust in the ONDC Network

The DSCI submitted a detailed response to the Open Network Digital Commerce consultation paper on **"Building trust in the ONDC Network" in September 2022**. The submission addressed critical gaps in digital trust considerations and provided comprehensive recommendations to strengthen security and privacy frameworks within ONDC's decentralized architecture.

DSCI recognized ONDC's transformative potential as an interoperable network that promotes goods and services exchange without centralized operational control. The submission acknowledged ONDC's approach would enhance buyer and seller participation by providing backend architecture for efficient transactions across platforms, lowering entry barriers and enhancing competition through greater specialization in e-commerce value chains.

The primary concern raised by DSCI centred on the consultation paper's narrow focus on traditional commercial trust elements while overlooking crucial aspects of digital trust, particularly data security and data privacy. The submission provided nine key recommendations to enhance trust in ONDC. DSCI advocated for transparent onboarding processes that ensured real identities of network participants, incorporating architectural ideas that promised higher assurance levels, enhanced authentication security, and strong authorization while removing friction from onboarding and transaction processing.

The submission emphasized the critical need for security and privacy integration in design phases, careful integration in development operations, and maintaining strong postures against evolving threats. Given ONDC's focus on inclusively onboarding small and medium businesses and neighbourhood retailers, DSCI stressed that the platform needed to take significant responsibility for maintaining decentralized architecture, as these smaller participants might lack adequate resources and knowledge to maintain security and privacy standards independently.

The submission highlighted specific technical recommendations for fraud prevention, including layered security approaches starting with advanced risk-assessment tools using machine learning and artificial intelligence to analyse consumer data during transactions. DSCI recommended real-time risk-assessment scoring systems, risk-based adaptive authentication methods, and comprehensive risk management frameworks that addressed channel risks across mobile, online, staff, terminal, and network environments. Additional fraud mitigation tools included Address Verification Systems, Payment Card Industry security standards adherence, and strong password requirements.

DSCI made its observation on the inherent challenges in ONDC's decentralized model, particularly regarding scalability and participant management. DSCI also raised concerns about data ownership and control within ONDC's framework. The submission noted consumers' perceived lack of control over personal information access during online navigation processes posed significant trust challenges, particularly given ONDC's decentralized model and unclear data ownership structures. DSCI

recommended that ONDC's network policy clarify data privacy and security aspects to acquire consumer trust throughout transaction lifecycles.

For search and discovery processes, DSCI emphasized the need for algorithmic accountability and ethical AI principles to mitigate bias risks during development phases. Strong recommendations were made on establishing verification mechanisms to ensure genuine search results from authorized sellers and transparent disclosure requirements covering platform information, network participant details, goods and services information, privacy policies, and data collection, processing, storage, and sharing practices.

Regarding payments and settlements, DSCI noted that ONDC's system remained susceptible to structural and technological challenges in digital payment systems, including cyber-frauds, transaction costs, communication infrastructure issues, and adoption barriers. The organization recommended encouraging network participants to practice cyber hygiene, including regular software updates, avoiding public Wi-Fi networks, changing passwords regularly, recognizing phishing scams, and installing dual-factor authentication and biometric solutions.

DSCI expressed concerns about ONDC's Issue and Grievance Management system, which relies heavily on self-regulation by participants. The submission recommended that ONDC should take responsibility for overseeing the IGM process until comprehensive network policies and open data initiatives were fully established. Additionally, DSCI recommended automating monitoring systems using AI and machine learning techniques to track transaction conformance with network policies. Strong recommendations were made advocating for leveraging policy-based automated governance through orchestration and observability techniques.

DSCI's comprehensive response demonstrated deep understanding of the complexities involved in building trust within decentralized digital commerce networks. The submission balanced recognition of ONDC's innovative potential with practical concerns about security, privacy, and governance challenges inherent in open network architectures. Overall, the recommendations provided actionable frameworks for addressing digital trust gaps while supporting ONDC's objectives of democratizing e-commerce access and promoting fair competition in India's digital marketplace.