Doc: MSD 05 (23519)/C
ISO 19626-1: 2020

For Comments Only

Draft Indian Standard

Processes, Data Elements and Documents in Commerce, Industry and Administration — Trusted Communication Platforms for Electronic Documents — Part 1: Fundamentals

ICS 35.240.63

Not to be reproduced without the permission of BIS or used as Standard	**Last Date for receipt of Comments is October 2023**

NATIONAL FOREWORD

(Formal clauses to be added later on)

The text of the International Standard has been approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as `Indian Standard'.

Annexes A, B and C are for information only.

Note: The technical content of the document is not available on website. For details, please refer the corresponding ISO 19626-1 : 2020 or kindly contact:

Head
Management and Systems Department
Bureau of Indian Standards
Manak Bhawan, 9, B.S. Zafar Marg
New Delhi – 110 002
Email: msd@bis.org.in
Telephone/Fax: 011-23231106

Scope

This document defines the requirements about trusted communication in legal, administrative and technical considerations. This document shows a TCP system architecture to guarantee trusted communication and promote trusted services by providing trusted communication evidence as the proof.

This document focuses on TCP at the view of 7th application layer of OSI (Open Systems Interconnection) Reference Model.

The audiences are the policy makers for IT innovation such as dematerialization, legal experts regarding electronic activities, IT planners for single windows and secure transactions, IT service providers related to distributed networking and ledger, trusted system auditors, trusted communication concerned parties and so on.

Introduction

Amidst the big flow of openness and integration in the world's economy, ICT (information & communications technology) is used as a means for innovation in productivity and connectivity. Since the value chain of products and services gets enlarged globally, business collaborations need electronic communications to be secure in an open and distributed environment. In this sense, electronic documents are asked for as a proof of business communications, meanwhile legal evidence or legal force is required.

However, it can be difficult to recognize electronic documents as the original source. There exist cases where many processes rely only on paper documents, even though electronic documents are widely implemented in business processes. However, the reality is that even if electronic documents are properly communicated in business transactions, the final data output may be on paper and stored in the form of printed copies as legal evidences for a long-term period. As such, this coexisting environment of electronic documents and paper documents causes breakup of the value chain, resulting in sluggish productivity, inefficiency, cost increase and offset of the benefit obtainable from the ICT. To improve these situations, therefore, it is essential to draw out a dematerializing solution that can guarantee the trustworthiness of electronically communicated document given legal evidence.

A dematerializing solution should meet with legal considerations about electronically communicated documents. However, this solution is not easy, because electronic communication itself includes the uncertainties from network failure and the electronic document itself is insufficient in safeguarding the integrity during its lifecycle. In the meantime, the problem due to repudiation, inadvertent disclosure or tamper has been regarded too sensitive to finalize the dematerialization solution related to business transactions as well as diverse governmental services, because it can protentially be embroiled into legal dispute or conflicts.

This document focuses on how to enhance trusted communication in an open and distributed environment. The trusted communication means electronic communication can ensure integrity and non-repudiation of electronic transactions by a trusted third party in a dematerialization manner under the guidance of UNCITRAL (United Nations Commission on International Trade

Law). For this open and distributed environment, at first, it should be able to minimize some innate difficulties around dematerialization. To solve these difficulties, this document approaches a solution by forming the trusted third party oriented and mutually trusted relationship among concerned stakeholders and implementing a shared platform which is accountable and traceable. In detail, a trusted communication platform needs to be able to keep the evidence about electronically communicated documents in a reliable and trustworthy manner. To achieve that, a new approach is required because the existing ICT environment has some limits for the trusted communication in the following aspects;

- Although an EDI (electronic data interchange) transaction can provide legal evidence about interchanged electronic documents according to the EDI syntax rule, it has limitations allowed only on closed users of EDI network and pre-defined processes of EDI semantics. And in the case of Internet, no matter what business transactions are securely communicated, it is difficult to recognize the legitimacy of communications carried out in other authentication sytems. In this sense this document sets up a refined dematerializing process allowable under the open and distributed ICT environment, which is applicable to the trusted communication like electronic trade, electronic administration, e-business and so on.
- The security technology has been used as a core technology for secured electronic documents. However, it is not enough to maintain the dematerialization of electronic documents, because the integrity is easy to be broken in the aspect of the valid period of security. In this sense this document brings up a new way that can secure the authenticity of the trusted communication evidence for a long period of time needed as legal evidences.
- IT services under an open environment can not easily identify the originality of electronic communications by accounting for the communication context, that is originator, addressee(s), communication time and so on. Regarding the uncertainties such as modification, falseness or bleach over electronically communicated documents, it is not easy to identify and ask for whose liability it is among multiple stakeholders. Moreover, if the block chain are to be applied across the supply chain, there is a need of trusted communication for seamless connectivity. In this sense, this document can make business transactions accountable and reliable and consequently promote trusted IT services.

An evidence generated via a trusted communication platform can account for the truth of e-communication activities and facilities trusted communication services.