INTERNATIONAL STANDARD

ISO 19626-1

First edition
2020-03

Processes, data elements and documents in commerce, industry and administration — Trusted communication platforms for electronic documents —

Part 1: **Fundamentals**

Processus, éléments d'informations et documents dans le commerce, l'industrie et l'administration — Plates-formes de communication sécurisées pour documents électroniques —

Partie 1: Généralités

Reference number
ISO 19626-1:2020(E)

© ISO 2020



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Trusted communication **4**
4.1 Overview 4
4.2 Legal considerations 5
4.2.1 General 5
4.2.2 Certainty of communication 6
4.2.3 Completeness of communication delivery 7
4.2.4 Confidentiality of communication delivery 7
4.3 Administrative requirements 8
4.3.1 General 8
4.3.2 Trusted communication platform service provider (TCPSP) 8
4.3.3 TCP main agreement 8
4.3.4 TCP client agreement 9
5 Trusted communication platform (TCP) **10**
5.1 Overview 10
5.2 TCP system architecture 11
5.3 TCP system requirements 12
5.3.1 General 12
5.3.2 TCP confidentiality 12
5.3.3 TCP authenticity 13
5.3.4 TCP reliability 13
5.3.5 TCP accountability 14
5.3.6 TCP portability 14
5.4 TCP system rules 15
5.5 TCP communication 15
5.5.1 TCP communication overview 15
5.5.2 Secure envelope 17
5.5.3 TCP message package 18
5.5.4 TCPSPs' communication binding 19
6 Trusted communication evidence (TCE) **21**
6.1 TCE generation 21
6.2 Evidential procedure 23
6.3 TCE custody 24
6.3.1 General 24
6.3.2 TCE Generation 24
6.3.3 Validation about TCE 25
6.3.4 Archiving of TCE 26
Annex A (informative) **Trusted communication reference model** **28**
Annex B (informative) **TCP main: quality and risk management** **29**
Annex C (informative) **TCPSPs' communication binding (an example)** **31**
Bibliography **35**

© ISO 2020 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 154, *Processes, data elements and documents in commerce, industry and administration*.

A list of all parts in the ISO 19626 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO 2020 – All rights reserved

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 blockchain are to be applied across the

© ISO 2020 – All rights reserved

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.

© ISO 2020 – All rights reserved

Processes, data elements and documents in commerce, industry and administration — Trusted communication platforms for electronic documents —

Part 1: Fundamentals

1 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.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
addressee
identifiable *party* (3.12) or destination which is intended by the originator to receive the *electronic communication* (3.5), but does not include a *TCPSP* (3.20) acting as an intermediary with respect to that *trusted communication* (3.21)

Note 1 to entry: This definition is adapted from UNCITRAL 2007, United Nations Convention on the Use of Electronic Communications in International Contracts.

3.2
audit
procedure to verify whether a product, a process or a system conforms to socially accepted criteria or standards

© ISO 2020 – All rights reserved

3.3
communication
statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract

Note 1 to entry: This definition is adapted from UNCITRAL 2007, United Nations Convention on the Use of Electronic Communications in International Contracts.

3.4
dematerialization
movement of paper proofs into electronic proofs by the evidential system which can capture the evidence of communications and verify that it is *trusted communication* (3.21)

3.5
electronic communication
communication that the parties make by means of electronic documents

Note 1 to entry: This definition is adapted from UNCITRAL 2007, United Nations Convention on the Use of Electronic Communications in International Contracts.

3.6
entity
subject who intends to communicate using electronic documents in a trusted manner in the real world

3.7
non-repudiation of delivery
NRD
state of affairs that a *TCPSP* (3.20) provides the originator of the message with evidence that the message has beed delivered

Note 1 to entry: See ISO 9735-5 and ISO/IEC 13888-1.

3.8
non-repudiation of origin
NRO
state of affairs that guard against the originator of a message falsely denying having sent the message

Note 1 to entry: See ISO 9735-5 and ISO/IEC 13888-1.

3.9
non-repudiation of receipt
NRR
state of affairs that guard against the recipient of a message falsely denying having received the message

Note 1 to entry: See ISO 9735-5 and ISO/IEC 13888-1.

3.10
non-repudiation of submission
NRS
state of affairs that a *TCPSP* (3.20) provides the originator of the message with evidence that the message has been submitted for delivery to the recipient

Note 1 to entry: See ISO 13888-1.

© ISO 2020 – All rights reserved

3.11
originator of communication
identifiable *party* (3.12) or destination by which, or on whose behalf, the *electronic communication* (3.5) has been sent or generated prior to storage, if any, but it does not include a *TCPSP* (3.20) acting as an intermediary with respect to that *trusted communication* (3.21)

Note 1 to entry: This definition is adapted from UNCITRAL 2007, United Nations Convention on the Use of Electronic Communications in International Contracts.

3.12
party
person or organization that participates in a transaction as a direct stakeholder

3.13
TCP accountability
state of being capable of explaining the fulfilment of *trusted communication* (3.21)

Note 1 to entry: See ISO 7498-2, ISO 9735-5, ISO/IEC 13888-1, ISO 15489, ISO 16175-3 and ISO 17068.

3.14
TCP authenticity
quality of being real or true about e-communication.

Note 1 to entry: The deinition is adapted from IETF RFC 6818.

3.15
TCP communication client
system component which performs the related functions by the communication request of an *entity* (3.6) under the *TCP* (3.23) system

3.16
TCP communication server
system component which performs transmission and reception of e-documents by acting as an agency of the *TCP communication client* (3.15) to generate the evidence

3.17
TCP confidentiality
quality of keeping an electronic document confidential, without any leakage, while delivering the e-documents

3.18
TCP reliability
quality of being able to make certain guarantees about the successful transmission of the message for *trusted communication* (3.21)

3.19
TCP portability
state or quality of being transportable with other application system in an open system environment

3.20
TCP service provider
TCPSP
service provider or *trustee* (3.25) that operates *TCP communication server* (3.16) and client and plays the role and responsibility about *TCP* (3.23) service by complying with related regulations, requirements and/or technical standards

© ISO 2020 – All rights reserved

3.21
trusted communication
highly qualified *electronic communication* (3.5) including a secure, accountable and reliable transfer of electronic documents for the purpose of *dematerialization* (3.4) in the distributed business environments, by meeting legal considerations like certainty, completeness and confidentiality of communication

3.22
trusted communication evidence
TCE
evidence record captured from *trusted communication* (3.21)

3.23
trusted communication platform
TCP
service platform enabling *trusted communications* (3.21) for exchanging electronic documents on legal liability by an open architecture on an open network

3.24
trusted third party
TTP
highly qualified person or body that is recognized as being independent and neutral from the parties involved, as concerns the issue in question

Note 1 to entry: See ISO 17068.

3.25
trustee
person or organization to whom legal title to a property is entrusted to use for another's benefit

3.26
truster
supporter who accepts something as true

3.27
trustworthiness
quality of being dependable and reliable

Note 1 to entry: See ISO 17068.

4 Trusted communication

4.1 Overview

In the open Internet, to secure paperless communications and works, it is essentially required to foster the trust. A trusted communication shall be able to guarantee the equality of paper-based documents or works and the legality about electronic communications and contracts.

The method of electronic communication is not sufficient to promote paperless communications and works. Even though an electronic method transfers electronic documents, its paper copy can be preferred as a source of evidence during the legal retention period.

At this aspect, UNCITRAL formulates some legislative guidelines to facilitate the use of electronic communications in international contracts. It declares the non-differentiation principle about the electronic and the paper form and then provides the legal requirements of the writing, the signature and the original form for electronic communication.

Paperless communication can be activated in the case of ensuring the authenticity of electronic documents related to communication. However, in an open Internet, different types of authentication technology can cause the dematerialization problem due to the interoperability. Any probable risks

© ISO 2020 – All rights reserved