INTERNATIONAL STANDARD

ISO 19626-2

First edition

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

Part 2: Applications

PROOF/ÉPREUVE

Reference number
ISO 19626-2:2020(E)

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

Published in Switzerland

Contents

Page

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*.

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.

Introduction

This document presents the TCP (trusted communication platform) system for trusted communication in the open and distributed ICT (information communication technology) environment, as a connected standard of ISO 19626-1.

The TCP system is a kind of middleware for connecting trusted communication in IoT (internet of things) or cloud environments, that delivers the information between humans, organizations, and devices by exchanging the e-documents via the TCP system components and stores the evidence of executed communication.

This document specifies the functionalities of processes and APIs (application programming interfaces) between TCP system components.

It intends to be described in the technology-neutral way in order that a TCP system can be implemented by applying various wire-wireless applied services and communication protocols used in the real world.

The key points that are implicated to this document are as follows.

a) The communication protocol used for inter-connection between TCP components is a core function of the application service layer in the distributed environment of wire and wireless communication.

The basic function of sending or receiving messages between the TCP system components compose the common communication interface to deliver message(s) in a distributed computing system of wire and wireless environment.

b) TCE (trusted communication evidence) can prove the trusted communication of in a TCP.

The TCP communication server executes reliable communication transactions, and create and store TCE as the proof in a way of non-repudiation between the communication participants.

c) A TCP system can be adequately ported to various kinds of business communication systems.

A TCP system is connected as a transmit or receive module between the e-business systems connected to be distributed with various work systems of B2B, e-government, and e-trade as well as the simple electronic communication systems to transmit contents directly using the address of sender or receiver (URLs, IP, address) such as the e-mail system as a related application system.

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

Part 2: Applications

1 Scope

As a connected standard of ISO 19626-1, this document defines the communication interactions between TCP system components and specifies their detailed interfaces— the processes and the APIs of the TCP system components.

It provides the common communication interface for deployment and implementation of the system components, and their functions in a specific technology-neutral way to those who consider applying and establishing a TCP system.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 19626-1, *Processes, data elements and documents in commerce, industry and administration — Trusted communication platforms for electronic documents — Part 1: Fundamentals*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 19626-1 and the following 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
blacklist
list of *e-identities* (3.3) of the originators who are proved having 'malicious intent'

Note 1 to entry: If a message is confirmed as *spam* (3.5), an e-identity who sent the spam is classified as a sender having 'malicious intent'.

Note 2 to entry: An addressee receiving a message from the originator in the blacklist can reject receiving the message.

3.2
characteristic information
unique identifying information to identify the entity in the offline (real) world such as a resident registration number, social security number, or identification number of an IoT device

3.3
e-identity
sole object to identify the entity who is the actual subject of communication activity under a TCP system

Note 1 to entry: In a TCP, it is the object which expresses the entity who is the actual subject of all activities including transmission, reception, and perusal (viewing or reading), etc. of e-documents after the electronic verification of identity.

3.4
e-identity ID
name that refers to an *e-identity* (3.3) identifying a value an e-identity gives itself for identification

Note 1 to entry: With the ID, the e-identity expresses itself and distinguishes itself from other e-identities.

3.5
spam
unsolicited email, which can carry malicious contents and/or scam messages

[SOURCE: ISO/IEC 27033-1:2015, 3.37, modified — "unsolicited emails" has been replaced with "unsolicited email".]

3.6
whitelist
list of trusted communication servers in a *TCP*

Note 1 to entry: If a communication server is proved that the one is secure technically and politically and complies with a standard and policy of the TCP, then TTP (trusted third party) directory server adds the one to its whitelist.

4 Relational architecture of TCP

4.1 Overview

ISO 19626-1 presents 2 types of 'TCP main' and 'TCP client' in system architecture. As a connected standard, this document enhances its relational architecture at the view of the interface.

As shown in Figure 1, once a transmitting entity (i.e, a sender) makes a delivery request to a receiving entity (i.e. a receiver), each of the components can be linked to one another through linkage interfaces, and the communication server is enabled to form an entrusted chain with a relying party. The pair-linked communication servers implement communication that can be entrusted, and through their interactions, generate TCE and can possess evidence in the TCE repository.

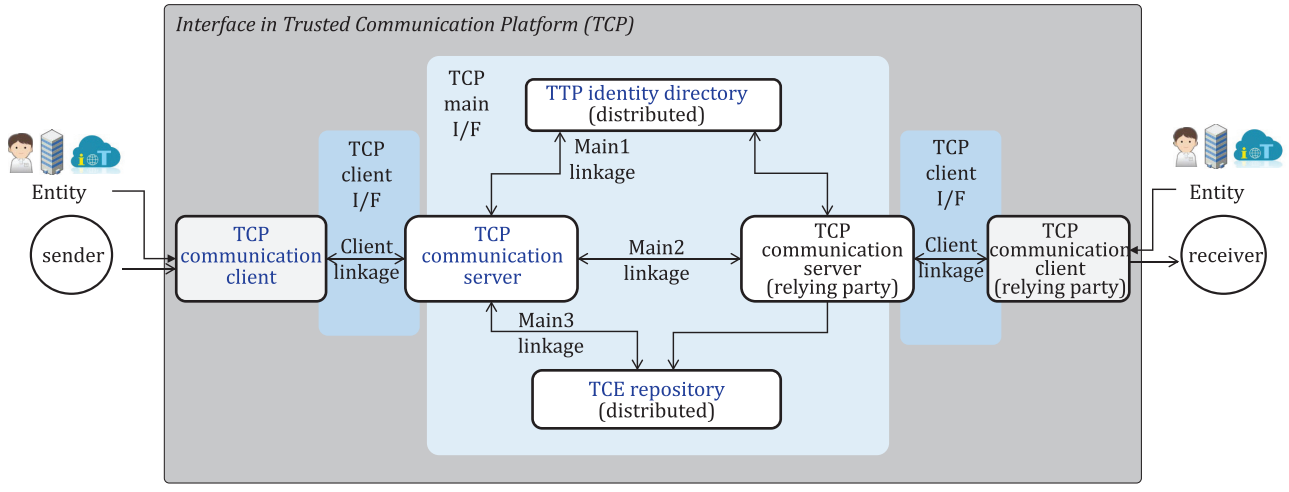

Figure 1 — TCP relational architecture

4.2 TCP relational architecture

Even if some communities intend to establish a TCP, they could not implement it in case their business and technical environments are different.

The particular authentication level, applied technology and communication protocol, etc. in each linkage need to be arranged properly by designing after classifying 'TCP main' and 'TCP client' even under various existing legacy system environments (refer to the ISO 19626-1:2020, 5.2). Figure 1 shows two interfaces.

a) TCP client interface

'TCP client interface' refers to an area inter-linked between a TCP communication client and a TCP communication server. Apart from various existing legacy system environments, a TCP communication client chooses and delegates a TCP communication server as its agent for trusted communication. At this point, 'TCP client interface' should be agreed and linked by the SLA (service level agreement) suggested by the communication server. Thus, in this interface, the communication server can function an agent of the communication client to transmit the requested e-document(s) in a trusted manner under a TCP architecture.

A TCP requires a standard interface for common linkage that a communication client and a server shall comply with. Then there are advantages of being able to provide convenience or efficiency of TCP operation to the communication clients. If a communication client wants to change its agent into the other communication server in a TCP, the communication client is able to change easily with it without being dependent on the proprietary interface of a specific communication server.

1) Client linkage: between a TCP communication client and a TCP communication server

— Once the entity gets to register its own e-identity by going through the process of verifying it from the TTP identity directory, this entity becomes a participant as a TCP communication client.

— A TCP communication client can participate in trusted communication after signing a service agreement provided by the communication server. This means the communication client doesn't perform the direct communication with the other communication client(s).

— A TCP communication client can delegate trusted communication after authentication of the TCP communication server in the PR3 (communication authentication process).

b) TCP main interface

'TCP main interface' refers to an area which performs practical trusted communication through three linkages that shall comply with a communication interface specification (see 6). 'TCP main' has the following types of linkage:

1) Main1 linkage: between a TCP communication server and a TTP identity directory

— For the communication server to send or receive e-documents on the behalf of communication client, information on the TCP communication server shall be registered in the TTP identity directory in the PR1 (communication server registration process).

— The newly registered TCP communication server shall get added to the whitelist as a trusted list in the identity directory. Then the identity directory shall notify the changed whitelist to the other registered communication servers in the PR2 (e-identity registration process).

— Communication server shall query to the identity directory in order to acquire and verify information on the relying party of reception in the PR4 (e-document transmitting process).

2) Main2 linkage: between TCP communication servers

— When a communication server transmits e-documents by inter-linking with the communication server of relying party, this communication server acts as a transmitting server.

— When a communication server has received the e-document, this communication server acts as a receiving server by processing it in the PR4 (e-document transmission process).

3) Main3 linkage: between a TCP communication server and a TCE repository

— Communication server(s) shall store the TCE generated after sending or receiving an e-document as evidence on the transactions of sending or receiving in the TCE repository in the PR6 (TCE preservation process).

— If verification on the communication of sending or receiving the e-document is necessary, TCE repository can verify the communication based on the stored TCE in the process of communication server verification.

4.3 Functionalities of TCP components

4.3.1 TTP identity directory

4.3.1.1 General

TTP identity directory provides a service to store and retrieve e-identity information on the entity after identifying and authenticating the entity participating in the trusted communication in a reliable method. The entity becomes a member of TCP as a communication client after registering an e-identity in the TTP identity directory. In one TCP, only one TTP identity directory that has e-identity information on all communication clients shall exist logically. In other words, even if the e-identity information is physically distributed or replicated information exists in various places, there should be only one integrated e-identity information logically and one shall be able to obtain the same information no matter when or by whom the information is searched or retrieved.

TTP identity directory provides the 5 functions defined in 4.3.1.2 to 4.3.1.6.

4.3.1.2 To register and manage trusted list of TCP communication server

— A TCP communication server shall perform the function to transmit or receive e-documents by receiving the request of the communication client. For doing it, this server shall be registered in the TTP identity directory.

— Before the TTP identity directory registers a TCP communication server, methods or procedures to verify functional security requirements, conformity of standards and interoperability shall be determined according to 'TCP main' policy. However, such a policy of the TTP identity directory shall reach a mutual agreement between the participants of TCP.

— After the communication server goes through verification on whether the concerned server is implemented by conforming to the standard and whether the necessary functional requirements are implemented, the network address of communication server and the information necessary for security, etc. shall be registered at the trusted list in the TTP identity directory.

— The trusted list of registered communication servers is managed as the whitelist and only the communication server listed in the whitelist can participate in the trusted communication. The whitelist consists of a trusted list of TCP communication servers in the process of communication server registration.

4.3.1.3 To identify entity

— TTP identity directory shall check and authenticate whether the information provided by the entity is identical to its actual information in the real world (e.g. if the entity is a person or an organization,

name or unique ID of the entity such as resident registration number, social security number or DUNS number, etc. and in case of a IoT device, it includes device ID, IP number and etc.) in the process of registering, modifying or deleting e-identity information.

— Criteria or methods for verifying the identity of an entity are determined according to the policy of the TTP identity directory and these shall be agreed between the participants who are performing trusted communication under the concerned TCP system.

4.3.1.4 To register and manage information of entity

— To perform trusted communication under a TCP system, the entity shall register e-identity information to the TTP identity directory.

— The entity may be a person or a conceptual subject such as a company, an organization, or IoT device, etc.

— For the entity to register its information, information on which communication server is used for sending or receiving e-documents in trusted mode is also necessary in addition to the basic information on the entity such as unique ID which represents an e-identity, entity name, and an ID commonly used in the real world (offline).

— In TCP, an entity is represented as an e-identity; and only an entity that has registered its e-identity may participate in the trusted communication of e-documents as a TCP communication client.

4.3.1.5 To search e-identity information

— If the transmitting client intends to send an e-document to a receiving client in TCP, the transmitting server which receives a request of sending an e-document from the transmitting client shall query to the TTP identity directory in order to obtain information on the receiving server which receives e-documents on the behalf of the receiving client.

— For this, the transmitting server requests to retrieve information which includes the network address of the receiving server used by the receiving client to the TTP identity directory using the e-identity ID value of the receiving client. After retrieving the requested information, the TTP identity directory returns the retrieved information to the transmitting server.

— Also, in order to verify whether the transmitting server that has sent the message is the legitimate communication server performing the role as an agent of transmission for the transmitting client at the time of receiving the message, the receiving server shall query on this to the TTP identity directory.

4.3.1.6 To handle spam messages, blacklist and whitelist

— Once the received message is determined as a spam message, the receiving client reports this message as a spam message to the TTP identity directory through the receiving server. The identity directory shall review the spam message status of this message after receiving the report of the spam message.

— Once the TTP identity directory determines the reported message as the spam message, the TTP identity directory shall add the originator (i.e., the e-identity of transmitting client) of the concerned message in blacklist and shall notify the updated blacklist to all communication servers in TCP. Unlike the whitelist managed as a list of communication servers, the blacklist is registered and managed as a list of e-identities.

— Criteria or procedures to decide whether the submitted report of the spam message is appropriate are determined according to the policy of the TTP identity directory and shall be agreed between TCPSPs (TCP service providers) who are performing trusted communication under the concerned TCP system.

4.3.2 TCP communication server

4.3.2.1 General

TCP communication server provides a service to send or receive e-documents using a trusted method by receiving a request of communication clients under a TCP system. All communication servers in one TCP shall be implemented according to mutually agreed transmission or reception protocols inside the TCP. Accordingly, all communication servers shall be verified in advance on whether the system operates by conforming to the standards agreed in TCP main and whether it is interoperable with other components in order to participate in TCP.

Methods or procedures to verify conformity with standards or interoperability on the communication server shall be determined by mutual agreement between the TCPSPs.

TCP communication server shall provide the functions defined in 4.3.2.2 to 4.3.2.11.

4.3.2.2 To register and manage TCP communication client

— TCP communication client shall sign on an agreement about the use of trusted transmission or reception service of e-documents provided by the TCP communication server to delegate actions of the trusted communication to the communication server.

— For doing this, the communication server shall provide a function for the communication client to apply for the use of services and a function to manage the information of communication clients with whom the communication server makes an agreement on the use of services.

— For the communication client to apply for the use of services to the communication server, a client shall be registered as an e-identity to the TTP identity directory and shall present a unique ID (i.e. e-identity ID) representing the e-identity registered to the identity directory when applying for the use of services.

— The communication server shall go through the process of verifying whether the connecting communication client currently is a legitimate owner of the e-identity ID presented by a communication client when applying for the use of services.

— After being registered to the TCP communication server properly, a TCP communication client will be able to use the trusted transmission or reception service of e-documents provided by the communication server.

4.3.2.3 To authenticate TCP communication client for requesting the services

— An authentication process on the communication client is absolutely necessary, so that communication server acts as an agent on the service in TCP by receiving a request from the communication client. In other words, the communication server shall know which e-identity the communication client requests the services with.

— To verify whether the client requesting usage of the services to the communication server is registered or not, the communication server shall perform authentication using various methods such as performing authentication using ID/PW, personal information or biometrics information of client.

— If a TCP client is authenticated successfully, the communication server, as an agent of communication client, performs the services related to the trusted communication of e-documents such as transmission, reception, perusal or a spam message report.

4.3.2.4 To create trusted chain for TCP communications

— Once the transmitting client requests transmission of messages to the transmitting server, the transmitting server shall authenticate the e-identity of the transmitting client first to prevent from deceiving the receiving client as if the transmitting client is another user.

— As the next step, the transmitting server requests the network address (such as IP address) of the receiving server to receive messages on behalf of the receiving client to the TTP identity directory using the e-identity ID of the receiving client presented by the transmitting client.

— The receiving server shall verify whether the transmitting server that has transmitted messages is the server properly registered in the whitelist of the TTP identity directory under TCP system.

4.3.2.5 To transmit messages

— The TCP communication server shall transmit the document by the request of the transmitting client to the receiving client using a trusted method.

  — For doing so, the communication server shall comply with all security and reliability requirements of the transmission process including proper verification of identity on the transmitting client, packaging of a trusted method on the delivered document, reliability on the identity information of the transmitting client, securing the integrity of transmitted messages, guaranteeing confidentiality in the process of trusted communication between the transmitting client or receiving client, and even the verification on whether the receiving client has received the e-document sent by the transmitting client.

    NOTE Integrity of transmitted message means to verify that the document transmitted is safely delivered to the receiving client from the transmitting client without being forged in the process of delivering document.

4.3.2.6 To receive messages

— The communication server as a receiving server shall respond after verifying whether the transmitted message from the transmitting server is a trusted message created according to the TCP transmission protocol.

— To make this possible, the receiving server shall verify the reliability on the transmitting client information in the received message, the integrity of the received message, confidentiality in the process of communication between the transmitting client and receiving client. etc. After verifying that the received message is trusted, it should secure justifiability and reliability on the reception of the message through the ACK (acknowledgment) for receipt confirmation.

4.3.2.7 To store and manage transmitted and received messages

— The communication server can safely store all messages transmitted or received under the TCP system by the request of the communication client.

— The communication server can set up the period to store transmitted or received messages and the scope of communication clients to access (search, browse or delete) the stored message according to the policy agreed at the time of concluding an agreement with the communication client.

— The communication server shall be managed to avoid the stored messages from getting leaked or damaged wrongfully by another communication client which is not the communication client for whom the access is permitted by the agreement with the communication client.

4.3.2.8 To handle spam message reports

— If the communication client requests to the communication server to report a specific received message as a spam message, the communication server reports the message as a spam to the TTP identity directory.

— Once the communication server-receives the examination result on the reported message as a spam from the TTP identity directory, the communication server shall notify this result to the communication client that had requested the report of the spam.

4.3.2.9 To create and deliver the NRR (non-repudiation of receipt)/NRD (non-repudiation of delivery) for receipt confirmation

— The receiving server shall create the NRR/NRD including the ACK signal to confirm that the receiving server has received the message at the time of receiving the message; and the NRR consists of the information of transmitting client, information of receiving client, transmitted date/time, received date and the information to prove that the contents of e-document is not forged (e.g. the hash value of e-document). NRD consists of the information of perusal confirmation (e.g. perused date/time, the hash value of perused e-document).

— In order that the transmitting server is able to get evidence that the e-document sent by the transmitting client is delivered properly to the receiving client, the receiving server shall deliver the NRR/NRD to the transmitting server instantly after creating the NRR/NRD.

4.3.2.10 To receive NRR/NRD and create TCE

— The transmitting server shall receive the NRR/NRD created by the receiving server after transmitting the e-document to complete the transmitting process successfully.

— The transmitting server shall verify whether the details on receipt confirmation included in the NRR/NRD is accurate, and whether this has been confirmed by the receiving server, based on the message of transmitting the e-document earlier.

— If the received NRR/NRD is valid, the transmitting server shall create TCE including this NRR/NRD.

4.3.2.11 To request storage and verification of TCE

— After creating the TCE including the NRR/NRD for receipt and/or perusal confirmation, the communication server participated in the trusted communication requests to store this into the TCE repository.

— The participants who have participated in communication or a third party that needs evidence shall request verification on the fact of sending or receiving e-document based on TCE stored in the TCE repository.

4.3.3 TCP communication client

4.3.3.1 General

'TCP communication client' means a component that performs the role of the entity's proxy under the TCP system for the entity to use the services of communication server to transmit or receive e-documents using the trusted method. Since a communication client may not transmit or receive e-documents, it shall use the concerned service after making sure to sign an agreement on the use of e-document transmission or reception service with TCP communication server in order to participate in the trusted communication.

TCP Communication client should provide the functions defined in 4.3.3.2 to 4.3.3.6.

4.3.3.2 To request authentication for using TCP communication services

— The communication client shall provide the function to deliver information for authentication to the communication server in order to get the approval of using the communication services provided by the communication server. For this, the communication client shall be registered to the communication server ahead.

— The communication client shall be allowed to use the functions such as requests to transmit or receive e-documents only in case of the communication client authenticated by the communication server.

4.3.3.3 To request transmission

— The transmitting client shall provide the function to make the transmission request information for transmitting e-documents to the receiving client.

— The transmitting client shall request the transmission of e-document by connecting to the transmitting server.

— The transmitting client shall provide the function to receive information of transmission status from the transmitting server after requesting the transmission of e-documents.

4.3.3.4 To get the received e-documents

— The receiving client shall provide the function to get the list of received messages, the detail information of specific message and the attached e-document by retrieving them from receiving server.

4.3.3.5 To request communication verification based on TCE

— When an entity desires to receive evidence to prove that the information of communication on the transmitted or received message is true, the communication client shall provide the function to deliver such a request to the communication server.

— The communication client that has received a request for communication verification from the entity shall request to verify the communication with the information of the communication (such as message ID) to the communication server and return the verification result received from TCE repository through the communication server.

4.3.3.6 To report spam messages

— The communication client shall provide a function to report spam messages if it (especially sending client) determines the received message as a spam message after perusing it.

— If a communication client (especially sending client) selects the received message and intents to report this as a spam message, it shall request to report the message as the spam message to the TTP identity directory through the communication server.

— The communication client (especially sending client) shall inquire the examination result of the spam status on the message which the communication client has reported as the spam message through the communication server.

4.3.4 TCE repository

4.3.4.1 General

'TCE repository' stores and manages the TCE which proves the fact of (communication) transmitting or receiving messages between communication servers. It plays a role of verifying the fact of communication and assigning trust on the verified information based on TCE when requested by someone else. TCE repository may be operated by one trusted third party or may be operated by getting distributed to TCPSPs. For example, most communication server might share TCE in each TCE repository such as blockchain. However, TCE repository shall have a precondition on the fact of being able to trust each other between all participants of TCP on the fact that the stored TCE is being safely managed from the threat of any forgery.

TCE repository should provide the functions defined in 4.3.4.2 to 4.3.2.3.

4.3.4.2 Storage and management of TCE

— After receiving and verifying the ACK signal including confirmation about information of communication obtained from the receiving server and creating TCE, the transmitting server shall