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 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

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.

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 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.

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

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.

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

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 and uncertainty also can be the obstacles for dematerialization. Therefore, it is necessaty to set up a qualified and trustworthy level for identifying the legal value for trusted communication.

Trusted communication can prove that its electronic document is a source of its communication evidence. In this sense, trusted communication provides a way of guaranteeing the quality of electronic communication and its proof verification system legally and technically. Trusted communication should also be applied to evidence based technogy such as blockchain.

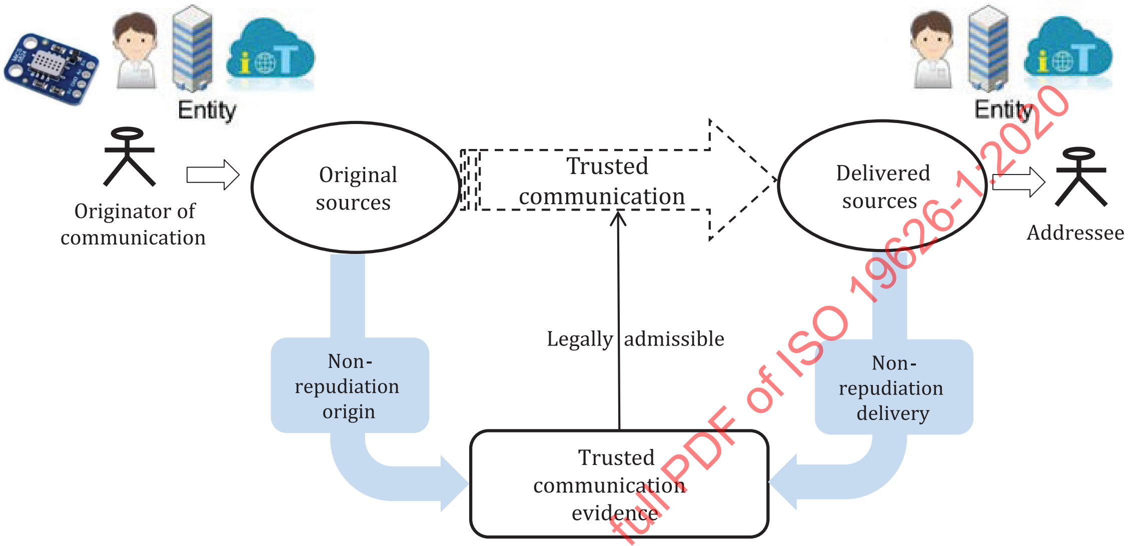

Figure 1 — Overview of a trusted communication

Figure 1 shows the trusted communication can be legally admitted by providing trusted communication evidence (TCE) which is composed of the non-deniable evicence of its origin and delivery. First, non-repudiation of origin (NRO) is the proof of the fact that all identies of communication originator and recipient(s) are authenticated/authorized in order to deliver e-documents (including originator's intention) in distributed environment. Non-repudiation of delivery (NRD) is evidence that the e-documents have been completely delivered from the originator to the addressee in the end-to-end communication. On the other hand, communication participants (or entities) includes machines as well as people like in Figure 1. In this regard, this document provides the TCP to ensure trusted communication and respond to any legal disputes and new technology changes.

4.2 Legal considerations

4.2.1 General

A communication is transmitted from the originator to the addressee. However, in the case of electronic communication, it delivers the electronic documents from the originator to the addressee and is executed in electronic transaction by the intermediary. This electronic transaction is a basic function in a business system which is either of simple type (such as e-mail systems) or complex type (many kinds of business systems or EDI including negotiation of contract, international transaction or e-government related works and so on).

However, there is a gap between electronic communication and legal definition. The term ”communication” is defined by UNCITRAL as "any 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”, whereas ”electronic communication” is referred to as only ‘its electronic means’. The legal group ascertains the factual existence and the content of communication between the parties in the context of formation of a contract. On the other hand, the technical group views actions of transmitting or receiving messages as proofs for transmission transactions. For example, ISO 8583-1 and ISO 20022-6 define electronic transaction as “an action of sending or receiving messages via an information communication network”.

This definitional gap causes disagreement about dematerialization. It means that even technically successful e-document cannot be easily admitted as a legal source about that transaction after passing a long term. The reason is that the electronic document has weak property to prove an original source through the successful communication. In order to remove this gap, electronic communication needs to provide its evidence which can be approved at legal aspects.

Therefore, this document sets up the requirements for the evidence of communication which shall be able to be approved at legal aspects. The following three requirements shall be met to fulfil trusted communication from legal aspects;

- the certainty of communication — whether an electronic communication is factually and certainly executed from/to communication partners;
- the completeness of communication — whether an electronic communication is successfully and completely executed by the intermediaries;
- the confidentiality of communication — whether an electronic communication is securely and confidentially executed from end to end.

These requirements provide a necessary and sufficient condition for fulfilling trusted communication. Herewith an evidence for meeting these requirements can be useful to provide legal admissibility.

4.2.2 Certainty of communication

In order to guaranttee the certainty of communication at legal aspects, its evidence can be duly approved that the communication parties and their business context are factual. To accomplish this, electronic communication methods shall be reliable and appropriate for the purpose for which the electronic communication was generated, or shall be proven to have fulfilled the function of identity and intention, either independently or together with other evidences. Therefore, trusted communication can include the following requirements for legal admissibility.

(1) Certainty about communication parties

In the case of non-face to face communication, it is important to confirm that communication parties are the very same persons and their communication contents have the very same own intentions in the communication context. In order to guarantee the certainty of communication parties, the evidence shall be able to capture the information of their authenticated identities like the following:

- Communication parties should be identifiable and authenticable that they shall be the right persons and their access should be authorized.

These methods or technologies are various for guaranteeing the certainty of communication parties. However, for a trusted communication, the authentication technology shall be recommended to use the same one or the mutually recognized one.

(2) Certainty about time and place

Trusted communication should be able to verify the fact of having been executed like the following:

- time of dispatch (leaving): time at which the sender has sent a message;

  Time information shall be adjusted and synchronized to the UTC (coordinated universal time) for protecting probable dispute about transmission.

- time of receipt: time at which the recipient has received the message;

  In case of communication transfer error (that is, the communication message is in a state of being left in an electronic communication system, not having been sent to the destination), time of receipt shall be considered acceptable.

— place at which the communication parties conduct business;

In general, the place designates the (physical or logical) location of the communication partners. Whereas, in the case of communication delivery, the place of intermediaries shall be considered together.

(3) certainty about communicated contents

The intentions of communication parties are represented in communication contents. Therefore, the integrity of the original form intended and written by parties should be verified as follows:

— about communication content which is created and signed by the originator of communication through a communication transaction;

NOTE A digitally signed document, in general, is an example of this. However, if without a signature, capturing information in a forensic way at transmission time can be considered as an evidence.

— about original form which can guarantee the authenticity and the integrity.

The integrity information such as hash value shall be captured and archived. This evidence is very useful to validate the custody of chain and trusted communication.

4.2.3 Completeness of communication delivery

It is generally approved that the intermediary can transfer or deliver electronic documents on behalf of communication partners (or clients). An intermediary should transfer and receive electronic documents under certain communication context to others. However, communication errors can occur from anywhere. On the other hand, some risks can come from the communication partner. Although an intermediary keeps its own logs, it can be difficult to confirm its completeness to the clients in the case of distributed communication systems like business supply chains. Therefore, trusted communication needs an intermediary to guarantee the completeness of its communication.

In order to verify the completeness of communication, all communication sections in distributed networks should provide the evidence about fulfilment of end-to-end communications. Also, its completeness should be able to be accepted by all participants of the communication, avoiding legal disputes.

From this perspective, the confirmation of the completeness can be shown as non-repudiation about the fulfilment of communication delivery by using digital signatures like followings;

— non-repudiation of origin (NRO);

— non-repudiation of submission (NRS);

— non-repudiation of reciept (NRR);

— non-repudiation of delivery (NRD).

4.2.4 Confidentiality of communication delivery

When the intermediary implements electronic communication, the confidentiality of its communication from end to end shall be ensured. Communication delivery should meet the following confidential requirements:

— The intermediaries shall transfer communication contents with encryption from the originator of communication (end) to the addressee (end). The content of communication shall be encrypted so that the communication information cannot be opened to others by any intermediary.

An originator can prefer to transfer his communication contents without encryption. But the intermediary shall transfer them with encryption.

— The intermediaries should protect the sensitive information such as personal information about communication parties. During or after transaction, their personal information should be protected from any infringement, violation or hacking etc. After completion of communication, the intermediary should protect the information from any unauthorized perusal and/or access to the content of communication.

4.3 Administrative requirements

4.3.1 General

An open and distributed environment is interlinked with a variety of business works, different services or diverse ICT environments. There are lots of interlinked and distributed communication systems such as single windows, supply chains, cross-borders, cross-industries and government projects, etc. This diversity can create the limitation in binding a chain of trust and introduce the problem of paperless communication. In this aspect, the trusted communication needs more managerial requirements in addition to the technical requirements in order to manage the trusted value chain among multiple service providers.

4.3.2 Trusted communication platform service provider (TCPSP)

TCPSP is a service provider that should mediate e-communications securely from the communication originator to recipient(s) concerned in the distributed environment such as registered e-mail service, cloud service or many kinds of service platforms. It is responsible for trusted communication in compliance with legal and technical requirements.

In the trusted communication, TCPSP shall be neutral, professional and responsible, and should provide trustworthy communicaton service as TTP (trusted third party), even in cross-border business and/or complex communication. In this sense, a TCPSP needs to reinforce the chain of trust among internal and external clients, as well as other TCPSPs (see Annex A). To do so, TCPSPs should maintain agreements needed for trusted communication.

As shown in Figure 2, a TCPSP (communication server) can play the role of a bridge between its client (communication client) and relying TCPSP (relying communication server). This means that TCPSP should reach two agreements such as "TCP main" and "TCP client".

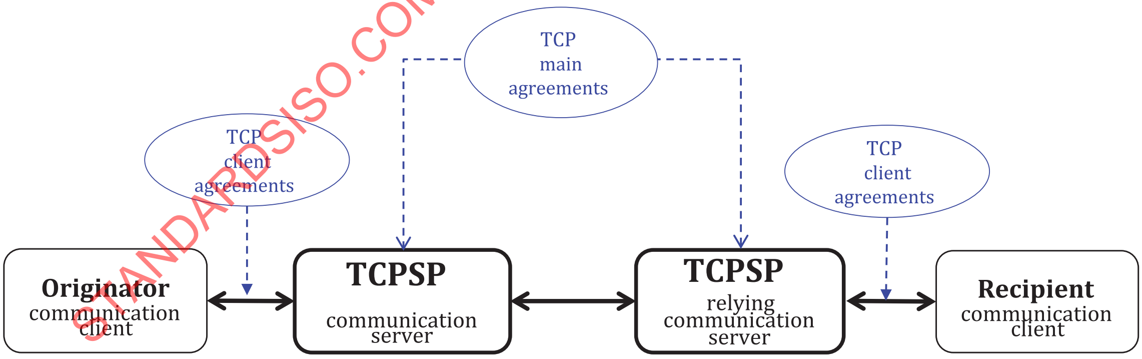

Figure 2 — TCPSP's role in trusted communication

4.3.3 TCP main agreement

"TCP main" is a mutual agreement between TCPSPs for the purpose of interoperability and quality under regulatory, technical condition or any economic community. It can formalize the qualified assured partnership and inter-connect trusted communication with TCPSPs.

“TCP main” can include agreements about policy, system, conformance, quality and risk. According to the change of business requirements, new technology and regulation, “TCP main” can be modified by regular agreements between TCPSPs. The followings are major “TCP main” issues to be considered.

(1) Policy requirements

- ownership of TCE,
- security policy to is applied to electronic document(s) and their transmission, including authentication, digital signature, cryptographic algorithm, key exchange and key management,
- confidentiality policy and management rule in end-to-end communication including secret key(s) management, encryption, enveloping, private information and legal liability,
- e-record policy including forensic capture, generation, retention and disposition of NRO, NRS, NRD, NRR, TCE(s) and e-documents, and
- other managements or actions.

(2) System management

- security facilities, secured storage, network security and functionality,
- system performance and load balancing,
- identity directory, distributed technology for sharing or federated e-identity directory and interconnection of other application systems or cloud services, and
- secured and reliable messaging and communication binding protocol and its interoperability.

(3) Conformance management

- testbed for interoperability between service providers, and
- portability to business service etc.

(4) Risk and quality management (see Annex B)

- risk management including role and responsibility and actions, and
- quality management including regular monitoring and auditing(tracking).

“TCP main” can be agreed in various common features depending on the communication social environment (national or economic community, etc.). However, due to limitations related to regional policy or different legacy systems, “TCP main” should apply open and secure technology and enhance the interoperability by adopting the following:

- technical interoperability guideline, and
- international standard.

4.3.4 TCP client agreement

“TCP client” means the mutual agreements between the TCPSP and its clients. It guarantees the partnership with the client. The TCPSP and the client should have an agreement such as a contract or SLA (service level agreement). The following are major “TCP client” issues to be considered:

- ownership about the client’s original communication,
- availability of TCE about the client’s original communication,
- confidentiality policy about privacy protection and legal liability,
- retention policy about TCE and e-document and legal liability,

— if necessary, key consignment policy, and,

— other managerial services.

5 Trusted communication platform (TCP)

5.1 Overview

For the purpose of legal liability, TCP should provide non-repudiation evidences with neutral and expertised involvement and include following features:

— it should include evidential functionality related to the cross confirmation of e-identities about originator and recipient, hash values of e-documents about before communication and after communication, receipt and TCEs about transmitting server and receiving server;

— it should include e-delivery functionality including evidential procedure to collect, generate and store it during the communication process.

In the real world, TCP types can be diverse, depending on whether it includes communication binding or not. Its simple type refers to mail delivery such as REM (registerd electronic mail) and its complex type supports business communication such as ERDS (electronic registered delivery service), supply chain services and so on.

NOTE 1 Complex communication includes the four-corner model which has multiple TCPSPs, fulfilling cross-border business transactions, trade, supply chains, healthcare, e-government services and so on.

The complex type involves the communication binding of multiple TCPSPs and needs to map some technologies such as security, distributed computing, record technology and the system interoperability. In this view, a technical reference model shows the technology map regarding TCP in Figure 3.

NOTE 2 Distributed computing technology such as cloud computing is defined as a model in which components located on networked computers communicate and coordinate their action by passing messages. This model is given in ISO/IEC 19941.

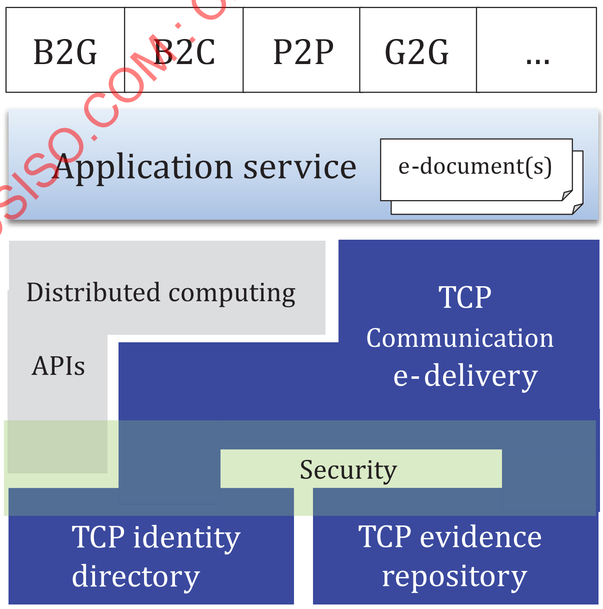

Figure 3 — TCP technical reference model

As shown in Figure 3, TCP's key functions are summarized as TCP communication e-delivery, TCP identity directory (including authentication and authorization function) and TCP evidence repositoty (including evidence custody). Security technology such as authentication (including signature, biometrics and etc) and cryptography (including encryption, hash, MAC and etc) is integrated into the communication network's transport layer and message layer in the process of e-communication and applied to them. Distributed computing technology is also applied to link with the application system and/or to access and share identity, metadata and evidence by using the application interface [including APIs (application programming interface)]. In addition, records technology is applied to capture, generate and store TCE by using the security technology (including non-repudiation). Thus, TCP can be regarded as a convergence technology that is a fusion of e-communication technology, security technology, records technology and distributed computing technology.

5.2 TCP system architecture

A TCP system in a distributed communication environment can fulfill end-to-end communication between its system components. TCPSP communication server must authenticate the identities of communication entities in a trustworthy manner and fulfil trusted communications without any communication error and networking failures by generating TCE. In this respect, TCP seems to be closely related to the communication funcationality in case of authorized P2P communication or private blockchain.

Figure 4 shows the TCP system architecture. The TCP system model consists of a pair of secured and interoperable communication systems (including each server and client) and two kinds of directories for identity and evidence. At this point, the TCP system can enhance trust chain and system interoperability through predefined TCP agreements such as “TCP main” and ”TCP client”. The system architecture is combined by requirements depending on “TCP main” and “TCP client” agreements.

In a distributed computing, a system component should function independently and interconnect with other components. In order to identify and interconnect with other system components in supply chains or cross-border transactions, TCP systems should adopt commonly recognizable digital signature technology among all the TCPSPs in a TCP.

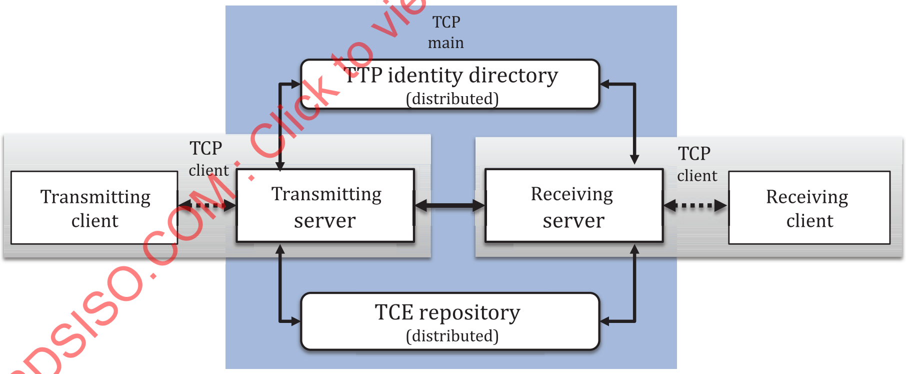

Figure 4 — TCP system architecture

In Figure 4, the TCP communication system plays the role of a transmission server/client or a receiving server/client depending on the direction of e-delivery. It should have the following major functions:

- to authenticate the identity of all of communication entity,
- to verify the integrity of the original source,
- to perform reliable messaging, and
- to generate and store TCE.

The TCP communication systems should interconnect with each other system components according to the following rules;

- server-to-server communication should use a common transmission module according to the “TCP main” agreement and requirements;

- server-to-client communication can use a common transmission module; but the client system can permit to expand various service interfaces such as mobile, sensor, cloud, etc according to the TCP client' circumstance;
- server-to-directory/repository communication can use a common transmission module.

In Figure 4, typology of TTP directory and TCE repository can be centralized or decentralized by adopting a kind of distributed technology as follows:

- the TTP identity directory shares the identity metadata and provides a white list and a black list. In order to share the identity information between TCPSPs, it can adopt an integrated, federated or distributed system selectively and should be operated efffectively; Its policy should be confirmed at the "TCP main" agreements and requirements between TCPSPs: and,
- the TCE repository which is storing the TCEs transferred from the communication server can be centralized or distributed by using DLT (distributed ledger technology); its policy should be confirmed at the "TCP main" agreements and requirements between TCPSPs.

5.3 TCP system requirements

5.3.1 General

The TCP should be operated to meet the following five system requirements in order to maintain legally admissible trusted communication and dematerialization mechanism in a distributed environment. The five requirements are confidentiality, authentication, reliability, accountability, and portability. These system requirements can be applied as the assessment of TCP system quality.

5.3.2 TCP confidentiality

In the distributed end-to-end communication, it is not easy to maintain the confidentiality between the originator and the recipient thoroughly. This is because the communication system can be connected in several kinds of internal systems or supply chain application systems. Thus, it is difficult to keep the confidentiality from the originator to the recipient. Nevertheless, some sensitive information such as privacy, personal information should be kept confidentiality thoroughly. In this sense, TCP confidentiality should be kept according to legal quideline, business secret and privacy protection.

In Figure 5, TCP confidentiality is technically classified into three levels according to the decryption path.

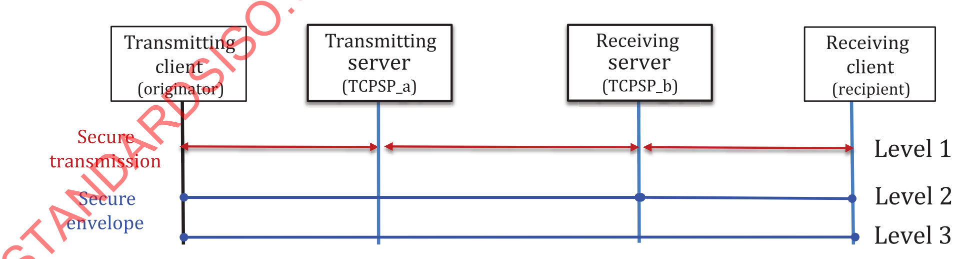
Transmitting client (originator)
Transmitting server (TCPSP_a)
Receiving server (TCPSP_b)
Receiving client (recipient)
Secure transmission
Secure envelope
Level 1
Level 2
Level 3

Figure 5 — TCP confidentiality

- **Secure transmission** (level 1) provides the confidentiality and authenticity during transmission but it has the limitation about ensuring the confidentiality beyond a pair of endpoints as shown in Figure 5. In the legal sense, level 1 plays a role to prevent external leakage. But because it is decoded at the end-point transmission path, TCP confidentiality should be strengthened through additional TCPSP's managerial rule in TCP main.
- **Secure transmission and secure envelope** (level 2, 3) In order to enhance confidentiality, TCP recommends that secure transmission use secure envelope of original contents. Level 2 has a decryption path at the receiving server. Level 3 is the most confidential way but it can be very vulnerable, if the information related to the recipient's secret key is lost or stolen.

In order to complement the technical weakness and ensure the quality, the following administrative considerations should be taken into account;

- **TCP main agreement:** Between TCPSPs, the confidentiality policy should clarify the role and responsibility (including legal liability), and technical and administrative provisions related security key, sensitive information such as privacy and business secret and respond to accidents and risks. The regular audits should be conducted to manage its quality.
- **TCP client agreement:** At SLA or contract, the client should check and agree on the liability of confidentiality of TCPSP. On the other hand, the client can consign his security key management for communication delivery to TCPSP.

In case TCPSP consigned the client's security information or for the purpose of risk management like TTPS's bankruptcy, succession or disaster, they are recommended to operate a security key management system (including hardware and software) in a separated and neutral manner.

5.3.3 TCP authenticity

TCP authentication is recommended by digital signature, but other authentication technologies that are agreed upon in a TCP main and client agreement can be permitted. TCP authenticity should be able to verify whether the in e-communication entity is true, whether the e-document to be delivered or TCE is the same as the original source (there is no change or tamper), and whether the TCP transport system is real by allowing security features. In this aspect, TCP authenticity can be divided into communication entity authenticity, secure server authenticity and e-document authenticity as follows:

- **Communication entity authenticity**: TCP system should be able to identify first all the TCP entities and then authenticate whether an entity is true or not. Identification is allowed by unique values such as id, distinguished name, biometric information, multi- factor information, hash value and so on.

  NOTE 1 In case there are multiple identity systems in a complex TCP type, TCP identification can be integrated by using distributed or federated ID technology.

- **Secure server authenticity**: TCP should verify that the communication system is a secure server that can transmit documents using the secure channel and that it is a TCP communication server.
- **Electronic document authenticity**: TCP system should be able to authenticate the document as it was transmitted during the end-to-end transmission by using hash or encryption and generate evidence. In addition, TCP may need long-term signature technology to maintain the authenticity of e-documents such as TCE for long term.

  NOTE 2 The long-term signature technology is adapted from the ISO 14533 series.

5.3.4 TCP reliability

In the legal sense, the reliability shall guarantee that the one and only communication delivery is free from any network failure. The TCP system shall be equipped with a reliable delivery service. In addition, it shall be able to prove the factuality of trusted communication. Many e-communication protocols, from EDI to ebMS or AS4, provide the following four basic delivery assurances:

- **AtLeastOnce**: Each message will be delivered to the recipient at least once. If a message cannot be delivered, an error must be raised by the transmitting server and/or the receiving server. Messages may be delivered to the recipient more than once (i.e. the recipient may get duplicate messages).
- **AtMostOnce**: Each message will be delivered to the recipient at most once. Messages might not be delivered to the recipient, but the recipient will never get duplicate messages.
- **ExactlyOnce**: Each message will be delivered to the recipient exactly once. If a message cannot be delivered, an error must be raised by the transmitting server and/or the receiving server. The recipient will never get duplicate messages.

- **InOrder**: Messages will be delivered from the receiving server to the recipient in the order that they are sent from the originator to the transmitting server. This assurance can be combined with any of the above assurances.

5.3.5 TCP accountability

TCP accountability means to collect, generate, transfer and store communication evidence which is non-repudiation in legal state by involving a trusted third party as a delivery agent.

- non-repudiation of origin (NRO);
- non-repudiation of submission (NRS);
- non-repudiation of receipt (NRR);
- non-repudiation of delivery (NRD).

TCPSP can acquire non-repudiation evidences as TTP by using the following techniques;

- verify the identity of the communication entity (digital signature),
- send the originator's electronic documents using secure envelope (hash, encryption),
- confirm the acknowledgement (reliable messaging), and
- capture the communication evidence forensically (WORM memory or ledger).

TCP accountability can generate TCE forensically by sending an extended envelope in the TCP message package signed with digital signature during end-to-end transmission.

In particular, TCP accountability should be able to provide selective acquisition of TCE in the case of sensitive information, business secret and so on. It means TCP accountability policy decides which work or business process needs to keep TCE, how long it should be stored and then disposed and so on. Therefore, TCE can be flexibly generated as needed in the business and legal aspects.

NOTE This rule is adapted from ISO 15489, ISO 16175-3 and ISO 17068.

5.3.6 TCP portability

The TCP system should be compatible and interfaced with a variety of IT systems and existing legacy systems under the open and distributed environment. Not only for mobile transmission but under the cloud environments, it should provide portability and interoperability with existing systems in a reliable manner.

A TCP system uses web service technology adopting appropriate security technology required in trusted communication in an open environment. In this open and secured environment, the TCP system can have flexible interactions with different kinds of application systems. This is explained through data portability, process portability and application portability like the following:

- **Data portability**: The TCP communication provides data portability to application systems or services by deliverling documents or sharing metadata in data interchange format such as XML, JSON and so on. In order to enhance data portability in case of cross-border business, its metadata using UN/CCL (core component library) is recommended.
- **Process portability**: In TCP communication, during the end-point message delivery process, a messaging transmission transaction (i.e., request-response) between the sender and the receiver is bound to a business transaction. At this aspect, TCP communication provides process portability within application systems. In particular, TCPSP should check and confirm security elements and, if necessary, capture the identification of process or procedure related to transmission transactions. It enables TCP effectively used for supply chain business.

— **Application portability**: TCP communication service using a web service can allow the external access. The TCP communication system components can provide the access to external application service via request and response service, in case of necessity. With this feature, TCP communication can provide application portability by interlinking various external supplementary services with API.

NOTE Application portability is adapted from ISO/IEC 17826, ISO /IEC 19941.

5.4 TCP system rules

All TCP components impact the whole quality of trusted communication. If a TCP component has a problem, this can impact and damage the others. Therefore, in order to entrust each other, TCP rules should be defined and closely observed. To allow trusted communication to be put into practice, the following specific rules shall be kept for mutual trusts among TCP components.

Rule 1: TCP communication servers shall deliver the encrypted sources in the reliable messaging methods from end to end clients. They should capture and generate TCE regarding the completion of trusted communication.

Rule 2: TCP intermediaries (or service providers, trustee) shall be made clear in terms of each role and responsibilities for trusted communication. They shall enter into the service agreements with its service assignor (truster). Each intermediary should have legal liability about its own service.

Rule 3: The TTP identity directory system shall be capable of rendering unique value in a unit of intermediary, organization or individual for the sake of legal accountability during the process of registration. All TTP identities should keep the confidentiality in the TTP identity directory system.

Rule 4: A TCP shall be able to apply the unified authentication methods and technique among TCPSPs and identity and evidence directories for the interoperability. However the TCPSP should be able to adopt flexible authentication methods for its own client services.

Rule 5: TCE metadata should be verifiable about the certainty of communication, confidentiality and completeness of communication delivery among communication concerned parties.

Rule 6: TCE shall be neutrally archived by TCPSP while maintaining its authenticity and integrity for a long period of time (as required such as the legal retention period). If requested from any communication partner (or originator of communication and addressee), it shall be able to prove trusted communication. If not requested, it should not be opened.

Rule 7: All TCP components shall maintain the required quality of trusted communication to provide against any fault in communication or custody due to various risks elements.

Rule 8: TCP shall provide its portability so as to support link with external systems.

5.5 TCP communication

5.5.1 TCP communication overview

TCP system components should provide TCP communication which can contain following security features;

- non-repudiation about the fact of sending and receiving,
- integrity and authenticity of transmitted messages,
- authorization about communication entity, and
- confidentiality of transmitting messages.

In Figure 6, TCP communication shows the process of end-to-end communication using secured transmission (confidentiality level 1) and secure enveloping (confidentiality level 2 or 3). It includes the following 5 major procedures.

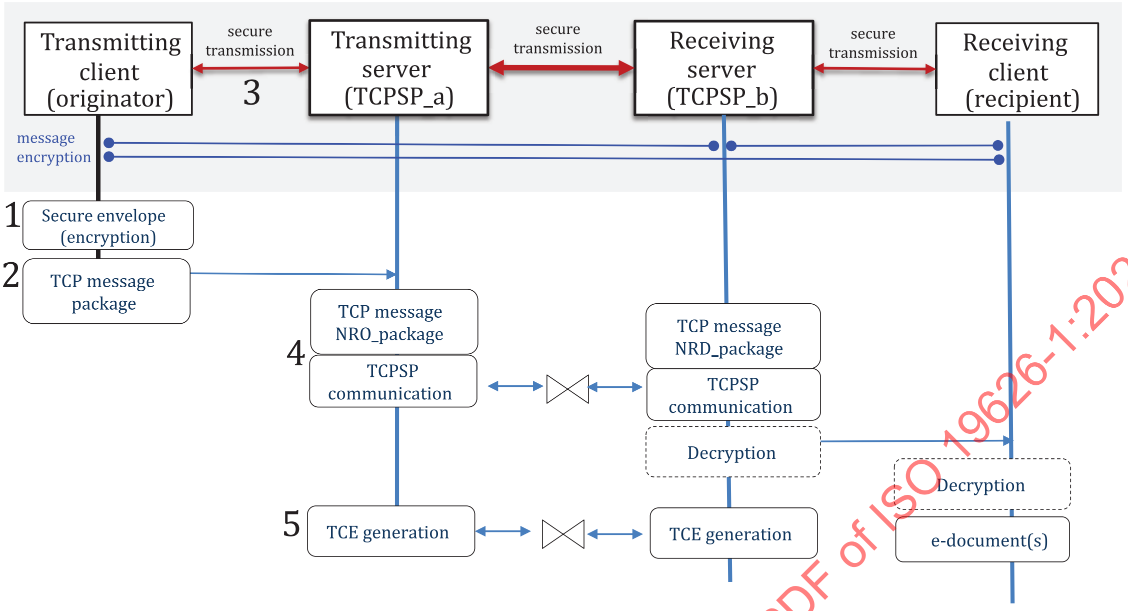

Figure 6 — TCP communication overview

(1) Secure envelope

All or some of the original source can be generated in secure envelope format to verify its confidentiality. The confidential policy related to secret key management should be set at TCP main. The hash value of the original source should be captured in order to verify the integrity of transmitted contents by using an encryption algorithm (symmetric or asymmetric).

NOTE 1 Secure envelope is adapted from IETF RFC 3852.

(2) TCP message package

TCP message package shall use the extended MIME container of SOAP envelope in order to account for the communication context and be transmitted in a reliable manner. The communication protocol for delivering e-documents such as ebMS, AS4 and so on should be agreed upon in TCP main.

NOTE 2 The reliable communication protocol for delivering e-documents is adapted from OASIS 2007.

(3) Secure transmission

Network transmission in the transport layer shall use a secure communication protocol such as SSL/TLS that can encrypt the contents and authenticate communication partners. Its cipher should be set according to TCP main.

NOTE 3 The secure transmission protocol is adapted from IETF RFC 5246.

(4) TCPSPs' communication binding

TCPSP communication should exchange messages between TCPSPs' communication servers. That is, TCPSPs' communication shall include communication binding on secured communication channel by delivering the information about trusted communication between transmitting server and receiving server. Before TCPSP's communication binding, TCP recommends to use agreed security elements such as cipher between TCPSPs for the simple binding and interoperable transmission. This document shows the example of the simple binding of communication collaboration by using ebCPP (ebXML collaboration protocol profile).

NOTE 4 An example of TCPSPs' communication protocol is adapted from OASIS 2002.

(5) TCE generation

TCE should be generated from delivering non-repudiation evidences during the communication process, validated and stored for the purpose of responding to legal disputes.

NOTE 5 It is adapted from ISO 7498-2, ISO 9735-5, ISO/IEC 13888-1.

5.5.2 Secure envelope

Secure envelope is beneficial to keep the confidentiality of all or some of the original source. An example of the secure envelope method is cryptographic message syntax (CMS) but any other equivalent methods are available. A TCP communication server resumes the responsibility for maintaining confidentiality and integrity as to all or some of the communication contents by creating encryption information. The following example of secured message using CMS is written by ASN.1. It pertains to evidence within EnvelopedData created in connection with content encrypted information, where hash information is included in EncryptedContentInfo.

NOTE This example is adapted from IETF RFC 3852.

EnvelopedData: A structure for conveying encrypted information, which includes key information for decryption in the side of recipient.

```
EnvelopedData :: SEQUENCE (
   originatorInfo [0] IMPLICIT OriginatorInfo OPTIONAL,
   recipientInfos RecipientInfos,
   encryptedContentInfo EncryptedContentInfo,
      unprotectedAttrs [1] IMPLICIT UnprotectedAttributes OPTIONAL)
```

— RecipientInfos includes key information for decryption in the side of recipient.

— In EncryptedContentInfo encrypted content information is inserted by applying the algorithm defined in TCP.

EncryptedContentInfo: A structure in which encrypted information is stored.

```
EncryptedContentInfo :: SEQUENCE (
   contentType ContentType,
   contentEncryptionAlgorithm ContentEncryptionAlgorithmIdentifier,
      encryptedContent [0] IMPLICIT EncryptedContent OPTIONAL)
```

— ContentType includes an identifier value that discriminates what information is contained in the content.

— In ContentEncryptionAlgorithm the algorithm that is actually applied for encryption is described.

— In EncryptedContent, the output (binary data) encrypted by ContentEncryptionAlgorithm is inserted.

RecipientInfo: A structure for items to be selected in regard of recipient's decryption information.

```
RecipientInfo :: CHOICE (
   Ktri KeyTransRecipientInfo,
   Kari [1] KeyAgreeRecipientInfo,
   Kekri [2] KEKRecipientInfo,
   pwri [3] PasswordRecipientInfo,
   ori [4] OtherRecipientInfo)
```

Provision of algorithm for encryption and decryption between the transmitter and the recipient shall be determined under the full extent of consent about trusted level between TCP service provider and auditor.

KeyTransRecipientInfo: A structure as per encrypted key information as key information for decryption selected by the recipient.

This example shows a case that the recipient selects KeyTransRecipientInfo.

```
KeyTransRecipientInfo :: SEQUENCE (
   rid RecipientIdentifier
   keyEncryptionAlgorithm KeyEncryptionAllgorithmidentifier,,
      encryptedKey EncryptedKey)
```

- In RecipientIdentifier a public key of the recipient is included.
- In KeyEncryptionAlgorithmIdentifier, information on the encryption algorithm for the recipient's private key is displayed.
- In EncryptedKey, the value of the recipient dedicated private key for decryption is included.

5.5.3 TCP message package

TCP message package refers to all structured communication containers which include transmission envelope, communication context and original contents. TCP message package applies single MIME containers for transmission. TCP message package is equivalent to SOAP envelope functions with security and reliability. Its well-structured package enables even complex trusted communications in an efficient and reliable way.

NOTE Message packaging is adapted from OASIS 2007.

Figure 7 shows the TCP message package. A characteristic of the TCP message package is to deliver the well-structured information bundle of trusted communication by a communication session. It structures the communication context information at the 1st contents part and transmitting communication contents at 2nd ~Nth contents parts.

The 1st content part is composed of message header (trusted communication context) and message body (TCE, non-repudiation info). Message header includes metadata of transmission such as communication party info (from, to), communication info and signature information of transmitting party (including certificate). Meanwhile, message body includes NRO or NRD for the request or respond depending on endpoint session.

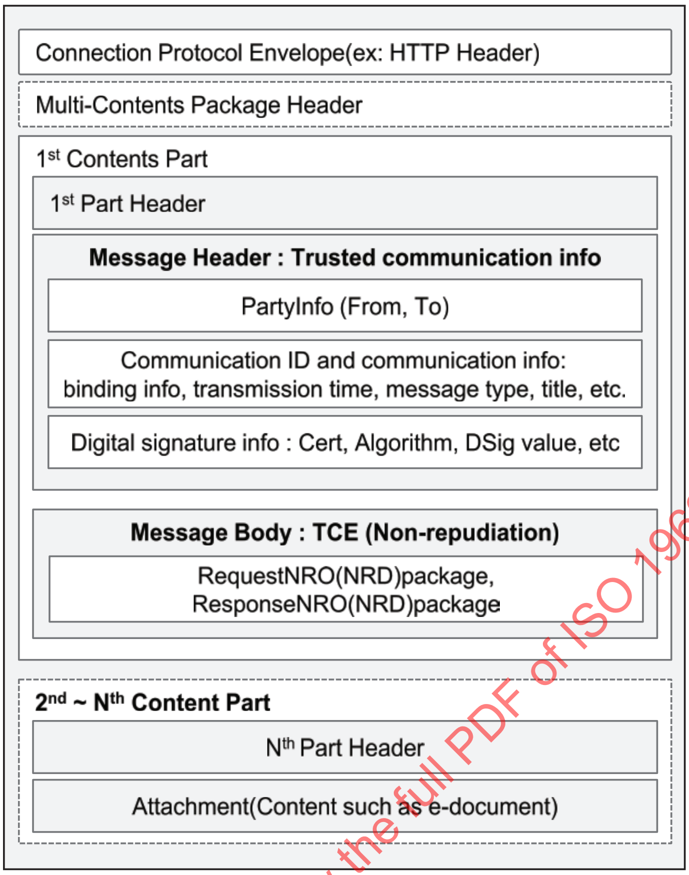
Connection Protocol Envelope(ex: HTTP Header)
Multi-Contents Package Header
1st Contents Part
1st Part Header
Message Header : Trusted communication info
PartyInfo (From, To)
Communication ID and communication info: binding info, transmission time, message type, title, etc.
Digital signature info : Cert, Algorithm, DSig value, etc
Message Body : TCE (Non-repudiation)
RequestNRO(NRD)package, ResponseNRO(NRD)package
2nd ~ Nth Content Part
Nth Part Header
Attachment(Content such as e-document)

Figure 7 — TCP message package

The 2nd ~Nth contents parts contain data set of the sender with the attached document. For the purpose of data and process portability, the 2nd contents part can contain data interchange format documents such as XML and JSON. Depending on confidentiality agreements, secured envelopes can be applied here. That is, the 2nd ~Nth contents parts can be varied depending on the contents source and confidentiality policy.

5.5.4 TCPSPs' communication binding

TCP communication is composed of end-to-end transmissions of TCP message packages. Among sessions, the TCPSPs' communication between the transmitting server and the receiving server is the most crucial. For this, it should check mutually security elements and then bind its communication collaboratively. Communication binding can be implemented by using distributed communication technology such as ebMS, SOAP, REST and so on. The following sample is a part of communication binding by using eb_cpp (related to ebMS).

NOTE eb_cpp is adapted from OASIS 2002.

The following is an example of communication binding via "secured delivery channel A" between TTPSP's transmitting server and receiving server. It confirms security elements such as cipher (which are mutually agreed in TCP main) and initiates the message binding between them.

```
< DeliveryChannel  docDeliveryId="docDelivery_A"
transportId="transport_A"  channelId="syncChannel_A">
</ DeliveryChannel>
< Transport  transportId="transport_A">
   < TransportSender>
      < TransportProtocol >HTTP</ TransportProtocol>
      < TransportClientSecurity>
         < TransportSecurityProtocol  >SSL/TLS</
TransportSecurityProtocol>
         < ClientCertificateRef  certId="TCPSP_a_ClientCert"/>
         < ServerSecurityDetailsRef
securityId="TCPSP_a_TransportSecurity"/>
      </ TransportClientSecurity>
   </ TransportSender>
   < TransportReceiver>
      < TransportProtocol  >HTTP</ TransportProtocol>
      < Endpoint uri="http: **** "/>
      < TransportServerSecurity>
         < TransportSecurityProtocol  >SSL/TLS</
TransportSecurityProtocol>
         < ServerCertificateRef  certId="TCPSP_a_ServerCert"/>
         < ClientSecurityDetailsRef
securityId="TCPSP_a_TransportSecurity"/>
      </ TransportServerSecurity>
   </ TransportReceiver>
</ Transport>
< DocDelivery  docDeliveryId="docDelivery_A">
   < ebXMLSenderBinding >
      < ReliableMessaging>< Retries>3</ Retries>< RetryInterval>PT1M</ RetryInterval>
      </ ReliableMessaging>
      < SenderNonRepudiation>
         < NonRepudiationProtocol> xmldsig#</ NonRepudiationProtocol>
         < HashFunction>sha256</ HashFunction>
         < SignatureAlgorithm>rsa</ SignatureAlgorithm>
         < SigningCertificateRef  certId="TCPSP_a_SigningCert"/>
      </ SenderNonRepudiation>
      < SenderDigitalEnvelope>
         < DigitalEnvelopeProtocol  >S/MIME</ DigitalEnvelopeProtocol>
         < EncryptionAlgorithm>AES128</ EncryptionAlgorithm>
         < EncryptionSecurityDetailsRef
securityId="TCPSP_a_MessageSecurity"/>
      </ SenderDigitalEnvelope>
   </ ebXMLSenderBinding>
   < ebXMLReceiverBinding >
      < ReliableMessaging>< Retries>3</ Retries>< RetryInterval>PT1M</ RetryInterval>
      </ ReliableMessaging>
      < ReceiverNonRepudiation>
         < NonRepudiationProtocol> xmldsig#</ NonRepudiationProtocol>
         < HashFunction>sha256</ HashFunction>
         < SignatureAlgorithm>rsa</ SignatureAlgorithm>
      < SigningSecurityDetailsRef  securityId="TCPSP_a_MessageSecurity"/>
   </ ReceiverNonRepudiation>
   < ReceiverDigitalEnvelope>
      < DigitalEnvelopeProtocol version="2.0">S/MIME</
DigitalEnvelopeProtocol>
      < EncryptionAlgorithm>AES128</ EncryptionAlgorithm>
      < EncryptionCertificateRef  certId="TCPSP_a_EncryptionCert"/>
   </ ReceiverDigitalEnvelope>
</ ebXMLReceiverBinding>
</ DocDelivery>
```

Meanwhile, during session, transmitting server should provide NRO message package (including NRS) and receiving severshould reply NRD message package (including NRR).

The following example of “cansend” function shows the binding “request NRO” from the transmitting server to the receiving server via secure delivery channel A. When a TCPSP transmitting server wants to bind to a receiving server via secure delivery channel A, each communication server should check the following security elements of the TCP message package (which are mutually agreed in TCP main) for the service binding:

- whether communication identities are authorized,
- whether a digital signature is applied as the tamper proof at the TCP message envelope,
- whether the e-document is authenticated with encryption or hash,
- whether the e-document is encrypted, and
- whether a message package provides non-reputational evidence.

Then the “cansend” function synchronizes communication between them delivery channel A and bind request-response action together.

```
<cansend>
   < ThisPartyActionBinding  packageId=" Request NROPackage "
action="request"
     id="request_response_a">
      < BusinessTransactionCharacteristics
         isAuthorizationRequired="true"
         isTamperProof="persistent"
         isAuthenticated="persistent"
         isConfidential="true"
         isNonRepudiationOriginalRequired="true"
         isNonRepudiationReceiptRequired="true"/>
      < ActionContext  requestOrResponseAction="request"
        businessTransactionActivity="request"
binaryCollaboration="request"/>
      < ChannelId>syncChannel_A</ ChannelId>
   </ ThisPartyActionBinding>
   < OtherPartyActionBinding>request_response_b</
OtherPartyActionBinding>
      < CanReceive>
      < ThisPartyActionBinding  packageId="SyncReplyNROPackage"
action="response"
        id="request_response_b">
         < BusinessTransactionCharacteristics
            isAuthorizationRequired="true"
            isTamperProof="persistent"
            isAuthenticated="persistent"
            isConfidential="true"
            isNonRepudiationOriginalRequired="true"
            isNonRepudiationReceiptRequired="true"/>
         < ActionContext  requestOrResponseAction="response"
           businessTransactionActivity="response"
binaryCollaboration="response"/>
         < ChannelId>syncChannel_A</ ChannelId>
      </ ThisPartyActionBinding>
         < OtherPartyActionBinding>request_response_a</
OtherPartyActionBinding>
      </ CanReceive>
</ CanSend>
```

The following is an example of TCE generation in Figure 8. It binds message package from TCPSP_a to TCPSP_b in the process of TCPSPs communication.

```
   < SimplePart  id="MsgNROHdr"  mimetype="text/xml"></ SimplePart>
   < SimplePart  id="Request"  mimetype="application/xml"></ SimplePart>
   < SimplePart  id="Response"  mimetype="application/xml"></ SimplePart>
   < Packaging  id="RequestNROPackage">
      < CompositeList>
         < Composite  id="RequestNROMsg"  mimetype="multipart/related"
           mimeparameters="type=text/xml">
         < Constituent  idref="MsgNROHdr"/>< Constituent
idref="Request"/>
         </ Composite>
      </ CompositeList>
   </ Packaging>
```

Annex C shows a whole example of TCPSPs’ communication by using ebCPP in case of ebMS communication protocol. But the other communication protocols can be applied.

6 Trusted communication evidence (TCE)

6.1 TCE generation

TCP can guarantee trusted communication by keeping TCE in a distributed communication environment. As a trusted third party, TCPSP should play an important role for delivering e-documents and generating TCE in a very secure and trustworthy manner for clients, application systems or distributed service. Non-repudiation evidence can be captured forensically by neutral intervention and technical expertise in a reliable manner and recorded in immutable meory such as WORM. TCE should be verified between communication partners and then generated, stored and disposed depending on the retention policy (which is agreed upon at TCP client or TCP main).

NOTE The evidential rule is adapted from ISO 17068, ISO15801 and ISO 16175-3.

Figure 8 shows TEC custody which is generated from NRO/NRS and NRR/NRD depending on a retention rule. TCE generation is provided by TCP communication between TCPSPs through service binding.

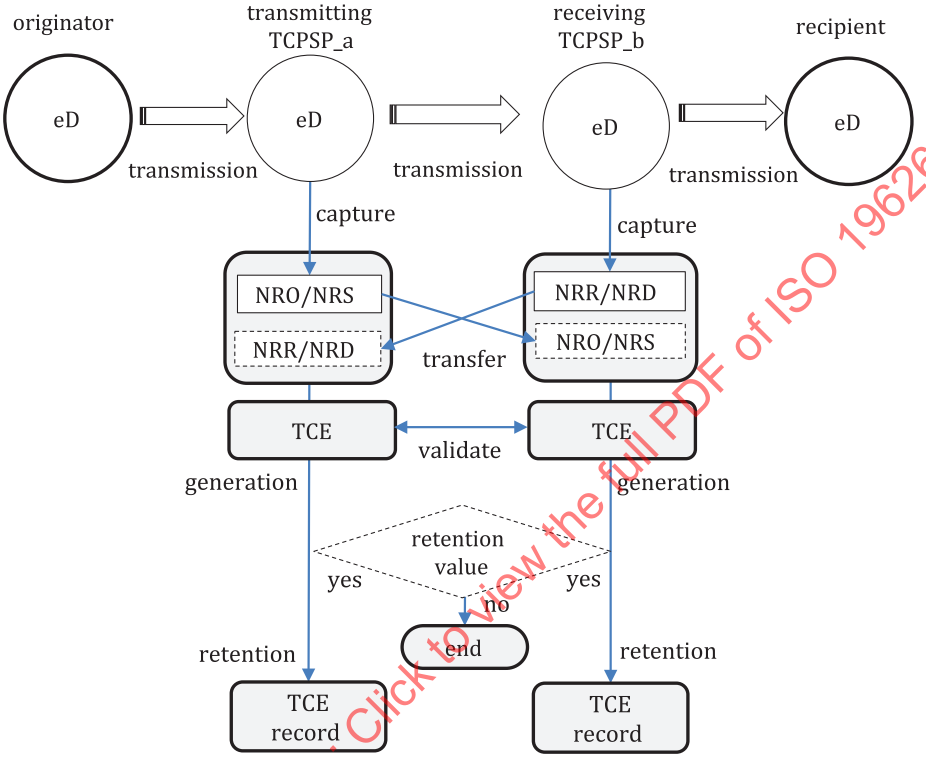

Figure 8 — TCE custody

(1) NRO/NRS information

- A TCPSP transmitting server can generate NRO captured from the originator's message envelopes and NRS captured submission time during transmission.
- NRO should be forensically captured. The communication entity information may be name, distinguished name, ID, address or hash. The authenticity of e-documents may be hash value, checksum or digital fingerprint by using symmetric or asymmetric encryption algorithm.

Table 1 shows an example of NRO package. Its metadata should be agreed upon in TCP main, taking legal requirements into consideration.

Table 1 — NRO/NRD data element

Data element	Type	Example	Cardinality
NRO/NRS ID	String	20180310_589_30240, R799fg27-13t6-3d5s-a9ct-d36e8tu95ew7	Optional
Originator ID	String	gildong.hong@nipa.kr, 5347146a-3528-4469-8ef7-9c346ab36d54	Mandatory

Table 1 *(continued)*

Data element	Type	Example	Cardinality
Recipient ID	String	soonsin.lee@kisa.or.kr, B366ff65-16c8-2d9d-a0ba-d76a2cc95ad2	Mandatory
Process hierarchy ID	String	urn : 1.1.5.3.1.18.2	Optional
Delivering contents ID	String	f73746a3-b65a-433f-a62b-8e5ee86aadf2	Mandatory
Submission time	String	2015.03.10T09:13:59:59;999z	Mandatory
Transmitting TCPSP ID	Sting	2295004872	Mandatory

(2) NRR/NRD information

- A TCPSP receiving server can generate its NRR/NRD by securing the acknowledgement received from the recipient (i.e. the client).
- NRR/NRD includes time information which is sent by the recipient. The following table shows metadata of NRR/NRD.

Table 2 shows an example of NRD package. Its metadata should be agreed in TCP main, taking legal requirements into consideration.

Table 2 — NRR/NRD data element

Data element	Type	Example	Cardinality
NRD content ID	String	S385zt69-46s7-2e9r-x8ab-u88x9gj39qk4	Optional
NRO content ID	String	R799fg27-13t6-3d5s-a9ct-d36e8tu95ew7	Optional
Recipient ID	String	soonsin.lee@kisa.or.kr, B366ff65-16c8-2d9d-a0ba-69z 6a2cc95ad2	Optional
Receiving time	String	2015.03.10T09:14:00:33;569z	Mandatory
Perusal time	String	2015.03.10T09:18:20:14;331z	Optional
Receiving TCPSP ID	String	3579074372	Mandatory

6.2 Evidential procedure

In the process of trusted communication, captured NRO, NRS, NRR and NRO can be generated into TCE. Figure 9 shows the forensic capturing process of TCE. Its process can be briefly described as having the following 4 phases:

- Phase 1: Capture authenticity information from the originator's message (NRO)
- Phase 2: Capture time of submission (NRS)
- Phase 3: Capture evidence from conformation of trusted delivery (NRR/NRD)
- Phase 4: Verify and then generate TCE according to retention rule

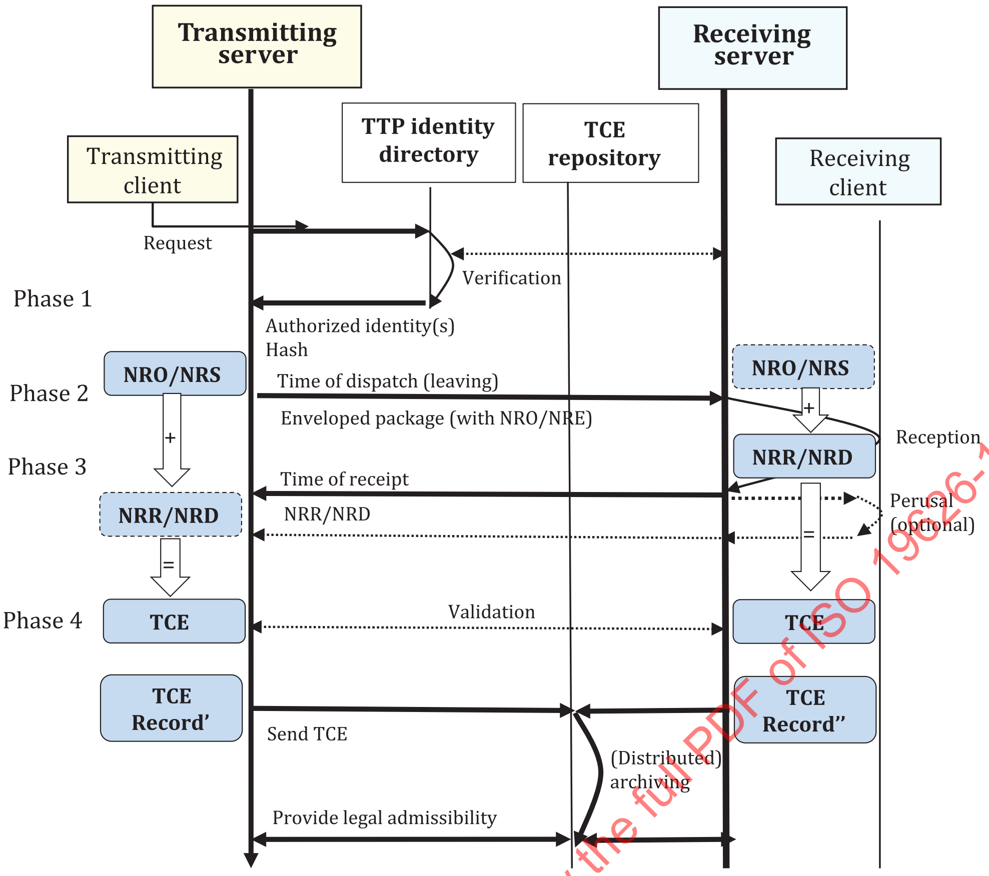

Figure 9 — Forensic capturing process of TCE

6.3 TCE custody

6.3.1 General

With regards to communication evidence information captured automatically through the procedures above, it should be validated as the TCE.

The transmitting unit should return it for the verification organization. Verification of this evidential weight shall be carried out by the neutral agency such as the receiving unit or another 3rd party organization and after verifying, its result should be delivered to the transmitting server.

After its validation, the transmitting unit signs it and then it is transferred to the evidence repository.

After generation, TCE should be archived ensuring authenticity, integrity, reliability and reusability and keeping evidential admissibility.

To preserve the evidential weight of TCE, it should be signed by an organization that is responsible for the evidence. In addition, it should be archived for the purpose of reusability of further providing evidence. That is, its communication context should be able to be retrieved and saved in a batch depending on its importance. Its level of quality should be required to prove its authenticity, non-repudiation and integrity with regular audit program, likely lawsuit and so on.

6.3.2 TCE Generation

A communication server should collect all non-repudiation evidences and transform them into TCE format. In order to validate the TCE, the transmitting server and the receiving server should compare the homogeniety of TCE by delivering each TCE. In case of discrepancy, communication error shall be detected again. After its confirmation about successful communiction, TCE should be generated under the following requirements:

- A TCE can generate the minimum necessary information from the NRO and the NRD, for the purpose of providing legal admissibility about trusted communication for a long period.
- A communication shall generate a TCE. Even when two or more documents are included in a communication, only one TCE shall be generated.
- In case TCE is generated by both the transmitting server and the receiving server, each TCE shall be cross-checked for uniformity between them immediately. Meanwhile, in case the mission of TCE generation can be consigned to a communication server (transmission server or receiving server), the TCE generation mechanism should be verifiable by an auditor or forensic system.
- After TCE validation, TCE should be generated in an evidence record format which does not allow any revision or change. In TCE generation, the following basic fields should be included;
  - TCE version,
  - TCE unique No.,
  - issuer (creator) of TCE,
  - issue date/time or timestamp of TCE,
  - TCP OID policy, and
  - proofs (content to be proven): the content collected as evidence of trusted communication that is collected as described above.

6.3.3 Validation about TCE

6.3.3.1 Verification of TCE format and its content

Format verification refers to a process that checks whether the format assessment of TCE conforms to the structure and value limitations defined by this document. When carrying out the verification of TCE format, the following should be checked;

- Are all requirements of the format of TCE satisfied?
- Is the version of the TCE format set appropriately?
- Is the serial number of the TCE format created in accordance with the rules?
- Is the date/time field of the TCE format created in accordance with the rules on generalized time?
- Is the TCE issuer identifiable in accordance with the rules?
- Is the policy on issue of TCE included?
- Does information on the sender and the receiver correctly match with each other?
- Is time information in accord with time field values within TCP envelope content?
- Is the communication identification value in accord with the ID value of TCP envelope content?
- Is the value of individual files within TCE in accord with the value of electronic document that was actually communicated?
- Is the hash value of individual files within TCE in accord with the hash value of electronic document that was actually communicated?

6.3.3.2 Verification about time information in TCE

The verification of TCE time is a process that checks whether each value on time set in TCE is normal at the point of reference for verification. It is necessary to check whether the following rules are met by comparing values of time fields set in TCE with the reference time values for verification.

- Transmission date/time ≤ receipt date/time + error range
- Receipt date/time ≤ perusal date/time + error range
- Perusal date/time ≤ date/time of issuing a certificate =< time of verifying a certificate

6.3.3.3 Verification of digital signature in TCE

To verify the integrity of TCE content, it is necessary to verify the electronic signature attached by the TCE issuer. This process is to verify whether the certificate of electronic signature attached in TCE is valid and whether it is the same as the information provided by TCE issuer. More specifically, it includes verification of the certificate's valid period, verification of disposal and trusted paths with CA certificates in the upper level.

After successful verification of its electronic signature, the mutual conformity should further be checked by comparing it with issuer name in TCE.

Once the successful verification of TCE issuer is achieved, the next step is to comparatively verify whether the signature of the TCE issuer is the same as that in the signature certificates contained in the white list of TCP identity directory. This step should be mandatory because it is necessary to confirm that the issuer who created the TCE belongs to TCP.

6.3.4 Archiving of TCE

A TCE resulting from the successful verification of its validity can be selectively retained depending on user-driven retention and disposal rules. At this point, it is important for a transmitting server to transfer TCE to TCP evidence repository without any injury. As soon as the TCE is transferred for its custody into TCP evidence repository, it shall send a confirmation message to the TCE assignor. Moreover, in case of security policy about TCE, TTP evidence repository can archive all or some of the security key from TCPSPs in the contract agreement and in a highly trustworthy manner.

NOTE This document covers only archiving of TCE. However, if communication contents and its TCE can be archived together, the dematerialization can be easily and clearly facilitated.

Table 3 shows a example of "trusted communication evidence".

Table 3 — An example of trusted communication evidence

Data element	Attribute	Example
TCE ID	TCE unique value	1234-5678-89-1234, nonce
	TCE type	transmission/ receiving/ perusal
Originator of communication	ID(address)	gildong.hongl@nipa.kr
	extension	R799fg27-13t6-3d5s-a9ct-d36e8tu95ew7
Addressee	ID(address)	yori.ko@kisa.or.kr
	extension	B366ff65-16c8-2d9d-a0ba-d76a2cc95ad2
Communication date/time	transmitting time	2015.03.10T09:14:00:33;569z
	receiving time	2015.03.10T09:15:00:18;431z
	perusal time	2015.03.10T09:18:20:14;331z

Table 3 *(continued)*

Data element	Attribute	Example
Communication contents	content title	Hello
	hash value (content)	nOczepEXEhtZGtpIXvRUiMnFutw
	attached file name	TCP overview.ppt
	hash value (attached file)	MnvWxtuiPhtoQRvTuROMSoptwP
TCE creation date/time	date or timestamp	2015.03.10T09:15:30:13;228z,
TCP OID	unique id	1.2.410.200032.6.1
TCE Issuer TCPSP's ID	unique id	37849249
Certificate of TCE Issuer	certificate	Sdiwrk382e9Pskfawiaasjlwawrql.....

Annex A
(informative)

Trusted communication reference model

Trusted communication needs to reinforce the chains of trust in this linter-linked and distributed environment. In order to reinforce trusted communication, it can be a solution for TTP to provide its trustworthy service.

Trusted communication is mutually inter-related by communication stakeholders as shown in Figure A.1. In trusted communication reference model, the trustee (service provider) plays an important role for interlinking chains of trust and requires a more qualified communication service as a trusted third party.

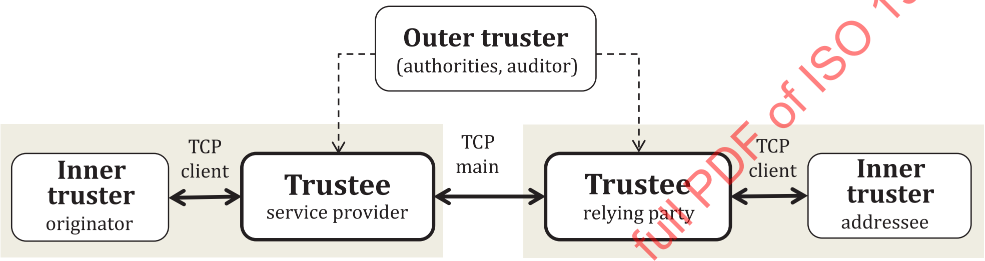

Figure A.1 — Trusted communication reference model

A TCP can be operated by correlating a certain level of trust between e-communication partners. The trusted communication reference model in Figure A.1 shows how to correlate the trust between them. However, in order to guarantee the trusted communication, not only the quality of direct e-communication but also its recognition from outer group like authorities and/or auditors should be considered. Even if there is any defection from any communication partner within a TCP, it can cause problems to trusted communication. Therefore, it is important to keep the entire agreement between all communication partners to guard it.

Annex B
(informative)

TCP main: quality and risk management

B.1 General

An auditor shall critically investigate the activities and performance of a trustee (that is, a trusted communication service provider) and report its findings to an assignor. The auditor should carry out such auditing activities based on fairness, objectivity and reliability.

The compliance audit refers to assuming the responsibility of auditing for compliance with the regulations as a whole, and specifically over the internal control system such as law compliance and risk management. The compliance auditor shall audit whether internal mandatory regulations comply with the prescribed procedure and standards regarding job execution and whether they are followed by executives and employees. If a violation is found, the compliance auditor will investigate such violation and report its result to an auditing committee.

The security audit provides the evidences that systems of consideration are free from danger and verified as effective and appropriate against threats, and that security measures are established as documented, understandable to each individual and properly implemented.

B.2 Risk management

Trustees face internal and external factors of uncertainties regarding trusted communication. These uncertainties are considered in the organization's objectives as "risk". The risk management is required to support experts responsible for trusted communication by quantifying risks that threaten trusted communication.

NOTE Principle of risk management is adapted from ISO 31010.

Most technical risks regarding trusted communication have been related to the information security technology during communication session and between platforms (end to end) and the vulnerability of electronic documents as an original source. If security is assessed through an ad hoc approach in a trustee, it frequently results in gaps to be mutually recognized as trusted communication. A more structured approach shall be reviewed to enhance the legal admissibility of electronic communication applied even to international contracts, and to assign risk factors (based on asset value of trustworthiness, system and electronic documents vulnerability and the likelihood of numerous kinds of attacks).

Once the risk analysis has been completed, its result needs to be reflected as part of the requirements for trusted communication. During review for this by stakeholders, considerations shall be given to reaching a balance between the achievable security effect and the risk evaluation compared with the cost of construction.

B.3 Quality management

To assure the quality of trusted communication from uncertain risks, it is necessary to qualify the state of the art of intermediary services in a certain period and audit their process and systems of capturing the evidence of communication. The quality of trusted communication should be obtained and assured by concerned parties such as the auditor, authority group, testing lab and so on according to the following procedure: plan, do, check and act.

NOTE Principle and procedure of quality management is adapted from ISO 9000.