# **INTERNATIONAL STANDARD**



First edition 2020-03

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

# Part 1: **Fundamentals**

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

Partie 1: Généralités



Reference number ISO 19626-1:2020(E)



#### © ISO 2020

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

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

Published in Switzerland

# Contents

Page

Introduction v   1 Scope 1   2 Normative references 1   3 Terms and definitions 1   4 Trusted communication 4   4.1 Overview 4   4.1 Overview 4   4.2 Legal considerations 5   4.2.1 General 5   4.2.2 Certainty of communication delivery 7   4.3 Administrative requirements 8   4.3.1 General 8   4.3.2 Trusted communication platform service provider (TCPSP) 8   4.3.3 TCP main agreement 9   5 Trusted communication platform (TCP) 10   5.1 Overview 10   5.2 TCP system architecture 11   5.3 TCP system architecture 12   5.3.1 General 12   5.3.3 TCP authenticity 13   5.4.4 TCP relability 13   5.5.5 TCP confidentiality 13   5.3.4 TCP relability 14   5.4 TCP system requirements 15   5.5.1 TCP contability 14   5.4 TCP system requirem	Fore	word		iv
1   Scope   1     2   Normative references   1     3   Terms and definitions   1     4   Trusted communication   4     4.1   Overview   4     4.2   Legal considerations   5     4.2.1   General   5     4.2.2   Certainty of communication delivery   7     4.2.3   Completeness of communication delivery   7     4.2.4   Confidentiality of communication delivery   7     4.3   Administrative requirements   8     4.3.1   General   8     4.3.2   Trusted communication platform Service provider (TCPSP)   8     4.3.3   TCP main agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system architecture   12     5.3.1   General   12     5.3.2   TCP confidentiality   12     5.3.3   TCP authenticity   13     5.4.4   TCP confidentiality   14     5.3.5   TCP communication overview	Intro	oductio	n	v
2   Normative references   1     3   Terms and definitions   1     4   Trusted communication   4     4.1   Overview   4     4.2   Legal considerations   5     4.2.1   General   5     4.2.2   Certainty of communication delivery   7     4.2.3   Completeness of communication delivery   7     4.3.4   Confidentiality of communication delivery   7     4.3.4   General   8     4.3.1   General   8     4.3.2   Trusted communication platform service provider (TCPSP)   8     4.3.3   TCP axin agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system requirements   12     5.3.1   General   12     5.3.3   TCP authenticity   13     5.3.4   TCP poolfidentiality   12     5.3.5   TCP ocontability   14     5.4.6   TCP accountability   13     5.5.1   TCP communication overview	1	Scop	e	
3 Terms and definitions   1     4 Trusted communication   4     4.1 Overview   4     4.2 Legal considerations   5     4.2.1 General   5     4.2.2 Certainty of communication delivery   7     4.2.3 Completeness of communication delivery   7     4.3.4 General   8     4.3.1 General   8     4.3.2 Trusted communication platform service provider (TCPSP)   8     4.3.3 TCP main agreement   9     5 Trusted communication platform (TCP)   10     5.1 Overview   10     5.2 TCP system requirements   12     5.3.1 General   12     5.3.2 TCP confidentiality   12     5.3.3 TCP system requirements   12     5.3.4 TCP reliability   13     5.3.5 TCP conduction   14     5.3.6 TCP portability   13     5.5.7 TCP communication overview   15     5.5.8 TCP communication overview   15     5.5.1 TCP communication overview   15     5.5.2 Secure envelope   17     5.5.3 TCP communication overview   15     5.5.4 TCPSPS' communication binding   19 </td <td>2</td> <td>Norr</td> <td>native references</td> <td>1</td>	2	Norr	native references	1
3   Terms and definitions   1     4   Trusted communication   4     4.1   Overview   4     4.2   Legal considerations   5     4.2.1   General   5     4.2.2   Certainty of communication delivery   7     4.2.3   Comfactiality of communication delivery   7     4.3.4   Confactiality of communication delivery   7     4.3.3   Confactiality of communication delivery   7     4.3.4   General   8     4.3.1   General   8     4.3.2   Trusted communication platform service provider (TCPSP)   8     4.3.3   TCP usted communication platform (TCP)   10     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system requirements   12     5.3.1   General   12     5.3.2   TCP confidentiality   12     5.3.3   TCP authenticity   13     5.4.4   TCP acountability   14     5.5.5   TCP acountability   14     5.5.4	2	Torr	and definitions	1
4   Trusted communication   4     4.1   Overview   4     4.2   Legal considerations   5     4.2.1   General   5     4.2.2   Certainty of communication   6     4.2.3   Completeness of communication delivery   7     4.3.4   Confidentiality of communication delivery   7     4.3.4   Confidentiality of communication delivery   7     4.3.4   General   8     4.3.1   General   8     4.3.3   TCP main agreement   8     4.3.4   TCP client agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system requirements   12     5.3.1   General   12     5.3.3   TCP actontiality   12     5.3.4   TCP proteibility   13     5.3.5   TCP actontability   14     5.4   TCP proteibility   14     5.5.1   TCP communication overview   15     5.5.2   Secure nucleace   17	3	Tern		<b>L</b>
4.1   Overview   4     4.2   Legal considerations   5     4.2.1   General   5     4.2.2   Certainty of communication delivery   7     4.2.3   Completeness of communication delivery   7     4.2.4   Confidentiality of communication delivery   7     4.3   Administrative requirements   8     4.3.1   General   8     4.3.2   Trusted communication platform service provider (TCPSP)   8     4.3.3   TCP client agreement   9     4.3.4   TCP client agreement   9     5.1   Overview   10     5.1   Overview   10     5.2   TCP system architecture   11     5.3   TCP confidentiality   12     5.3.1   General   12     5.3.2   TCP contability   13     5.3.5   TCP contability   13     5.4.7   TCP system rules   15     5.5.1   TCP communication overview   15     5.5.2   Secure envelope   17     5.5.3   TCP message package	4	Trus	ted communication	
4.2   Legar consuderations   5     4.2.1   General   5     4.2.2   Certainty of communication   6     4.2.3   Completeness of communication delivery   7     4.2.4   Confidentiality of communication delivery   7     4.2.4   Confidentiality of communication delivery   7     4.3   Administrative requirements   8     4.3.1   General   8     4.3.3   TCP main agreement   8     4.3.4   TCP client agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system requirements   12     5.3.1   General   12     5.3.3   TCP confidentiality   12     5.3.4   TCP portability   13     5.3.5   TCP confidentiality   14     5.4   TCP system rules   15     5.5.1   TCP communication overview   15     5.5.2   Secure envelope   15     5.5.4   TCP pers' communication overview   15     5.5.4   TCP		4.1	Uverview	
4.2.1   General   5     4.2.2   Completeness of communication delivery   7     4.2.4   Confidentiality of communication delivery   7     4.3   Administrative requirements.   8     4.3.1   General   8     4.3.1   General   8     4.3.1   General   8     4.3.2   Trusted communication platform service provider (TCPSP)   8     4.3.3   TCP dient agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system architecture   11     5.3   TCP confidentiality   12     5.3.1   General   12     5.3.2   TCP confidentiality   13     5.3.5   TCP conditiality   13     5.3.5   TCP accountability   14     5.3.6   TCP protability   14     5.5.7   TCP communication overview   15     5.5.8   Secure envelope   17     5.5.9   TCP communication overview   15     5.5.1   TCP message package		4.2	Legal considerations	
4.2.2   Certainty of communication delivery   7     4.2.4   Confidentiality of communication delivery   7     4.3   General   8     4.3.1   General   8     4.3.2   Trusted communication platform service provider (TCPSP)   8     4.3.3   TCP main agreement   8     4.3.4   TCP client agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system architecture   11     5.3   TCP enditentiality   12     5.3.1   General   12     5.3.1   General   12     5.3.3   TCP automatication   13     5.3.4   TCP reliability   13     5.3.5   TCP confidentiality   14     5.4   TCP system rules   15     5.5.5   TCP communication overview   15     5.5.2   Secure envelope   17     5.5.3   TCP proses age package   18     5.5.4   TCPSP' communication binding   19     6   Trusted communication ev			4.2.1 General	5
4.2.4   Confidentiality of communication delivery   7     4.3   Administrative requirements   8     4.3.1   General   8     4.3.2   Trusted communication platform service provider (TCPSP)   8     4.3.3   TCP main agreement   8     4.3.4   TCP client agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system architecture   11     5.3   General   12     5.3.1   General   12     5.3.2   TCP confidentiality   12     5.3.3   TCP active accountability   13     5.3.4   TCP prelability   13     5.3.5   TCP communication overview   15     5.5.5   TCP communication overview   15     5.5.1   TCP communication overview   15     5.5.2   Secure envelope   17     5.5.3   TCP message package   18     5.5.4   TCPSPs' communication binding   19     6   Trusted communication about TCE   24     6.3			4.2.2 Completeness of communication delivery	
4.3   Administrative requirements.   8     4.3.1   General   8     4.3.2   Trusted communication platform service provider (TCPSP)   8     4.3.3   TCP client agreement.   8     4.3.4   TCP client agreement.   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system requirements   12     5.3.1   General   12     5.3.2   TCP confidentiality   12     5.3.3   TCP authenticity   13     5.3.4   TCP portability   14     5.3.5   TCP communication overview   15     5.5.1   TCP orgenate plate pl			4.2.4 Confidentiality of communication delivery	
4.31   General   8     4.3.2   Trusted communication platform service provider (TCPSP)   8     4.3.3   TCP main agreement   8     4.3.4   TCP client agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system architecture   11     5.3.1   General   12     5.3.2   TCP confidentiality   12     5.3.3   TCP authenticity   13     5.3.4   TCP reliability   13     5.3.5   TCP accountability   13     5.3.6   TCP portability   14     5.4   TCP system rules   15     5.5   TCP communication overview   15     5.5.1   TCP communication overview   15     5.5.2   Secure envelope   17     5.5.3   TCP message package   18     5.5.4   TCP SPS' communication binding   19     6   Trusted communication evidence (TCE)   21     6.3   TCE generation   24     6.3.1   General   2		12	4.2.4 Confidentiality of confinumication derivery	
4.3.2Trusted communication platform service provider (TCPSP)84.3.3TCP main agreement84.3.4TCP client agreement95Trusted communication platform (TCP)105.1Overview105.2TCP system requirements125.3.1General125.3.2TCP confidentiality125.3.3TCP authenticity135.3.4TCP reliability135.3.5TCP communication155.5TCP communication155.5TCP communication155.5TCP communication155.5.1TCP communication155.5.2Secure envelope175.5.3TCP system rules185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.3TCE Generation216.3TCE Generation246.3.1General246.3.2TCE Generation246.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35		4.5	Automisti ative requirements	0 Q
4.3.2   TGP main agreement   8     4.3.4   TCP client agreement   9     5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system architecture   11     5.3   TCP considered in the system and the system architecture   11     5.3   TCP confidentiality   12     5.3.1   General   12     5.3.3   TCP confidentiality   12     5.3.4   TCP reliability   13     5.3.5   TCP accountability   13     5.3.5   TCP communication overview   15     5.5   TCP communication overview   15     5.5.1   TCP communication overview   15     5.5.2   Secure envelope   17     5.5.3   TCP message package   18     5.5.4   TCPSPs' communication binding   19     6   Trusted communication evidence (TCE)   21     6.3   TCE generation   21     6.3   TCE generation   24     6.3.1   General   24     6.3.2   TCE Generatio			4.3.2 Trusted communication platform service provider (TCDSD)	0 g
4.3.4TCP client agreement95Trusted communication platform (TCP)105.1Overview105.2TCP system architecture115.3TCP system requirements125.3.1General125.3.2TCP confidentiality125.3.3TCP authenticity135.3.4TCP reliability145.3.5TCP confidentiality145.3.6TCP portability145.3.7TCP accountability155.5TCP communication155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSys' communication binding196Trusted communication evidence (TCE)216.3TCE custody246.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) TCP main: quality and risk management29Annex C (informative) TCPS' communication binding (an example)31Bibliography35			4.3.2 TCP main agreement	0 g
5Trusted communication platform (TCP)105.1Overview105.2TCP system architecture115.3TCP system requirements125.3.1General125.3.2TCP confidentiality135.3.4TCP reliability135.3.5TCP contability145.4TCP system rules155.5TCP communication overview155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.3TCE generation216.3TCE custody246.3.1General246.3.2TCE Generation246.3.4Archiving of TCE256.3.4Archiving of TCE26Annex A (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			4.3.4 TCP client agreement	0 Q
5   Trusted communication platform (TCP)   10     5.1   Overview   10     5.2   TCP system architecture   11     5.3   TCP system requirements   12     5.3.1   General   12     5.3.2   TCP confidentiality   12     5.3.3   TCP authenticity   13     5.3.4   TCP reliability   13     5.3.5   TCP accountability   14     5.3.6   TCP portability   14     5.4   TCP system rules   15     5.5   TCP communication overview   15     5.5.1   TCP communication overview   15     5.5.2   Secure envelope   17     5.5.3   TCP message package   18     5.5.4   TCPSPs' communication binding   19     6   Trusted communication evidence (TCE)   21     6.1   TCE generation   21     6.2   Evidential procedure   23     6.3   TCE Generation   24     6.3.2   TCE Generation   24     6.3.4   Archiving of TCE   26  <			4.5.4 For cheft agreement	
5.1   Overview   10     5.2   TCP system architecture   11     5.3   TCP system requirements   12     5.3.1   General   12     5.3.2   TCP confidentiality   12     5.3.3   TCP authenticity   13     5.3.4   TCP reliability   13     5.3.5   TCP accountability   14     5.3.6   TCP portability   14     5.3.6   TCP portability   14     5.3.6   TCP communication overview   15     5.5   TCP communication overview   15     5.5.1   TCP message package   17     5.5.3   TCP message package   18     5.5.4   TCPSPS' communication binding   19     6   Trusted communication evidence (TCE)   21     6.1   TCE generation   21     6.2   Evidential procedure   23     6.3   TCE custody   24     6.3.1   General   24     6.3.2   TCE Generation   24     6.3.4   Archiving of TCE   25     6.3.4 <td>5</td> <td>Trus</td> <td>ted communication platform (TCP)</td> <td></td>	5	Trus	ted communication platform (TCP)	
5.2TCP system architecture115.3TCP system requirements125.3.1General125.3.2TCP confidentiality125.3.3TCP authenticity135.3.4TCP reliability135.3.5TCP accountability145.3.6TCP portability145.3.7TCP communication155.5TCP communication overview155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.4Archiving of TCE256.3.4Archiving of TCE26Annex A (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35		5.1	Overview	
5.3TCP system requirements125.3.1General125.3.2TCP confidentiality125.3.3TCP authenticity135.3.4TCP reliability135.3.5TCP accountability145.3.6TCP portability145.7TCP communication155.5TCP communication overview155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) TCP main: quality and risk management29Annex C (informative) TCPS' communication binding (an example)31Bibliography35		5.2	TCP system architecture	
5.3.1General125.3.2TCP confidentiality125.3.3TCP authenticity135.3.4TCP reliability135.3.5TCP accountability145.3.6TCP portability145.3.6TCP portability145.4TCP system rules155.5TCP communication155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex C (informative) TCPs' communication binding (an example)31Bibliography35		5.3	TCP system requirements	
5.3.2TCP confidentiality.125.3.3TCP authenticity.135.3.4TCP reliability.145.3.5TCP accountability.145.3.6TCP portability.145.3.6TCP portability.145.3.6TCP communication155.5TCP communication overview.155.5.1TCP communication overview.155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			5.3.1 General	
5.3.3TCP authenticity135.3.4TCP reliability135.3.5TCP accountability145.3.6TCP portability145.4TCP system rules155.5TCP communication overview155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			5.3.2 TCP confidentiality	
5.3.4ICP reliability135.3.5TCP accountability145.3.6TCP portability145.3.6TCP opticability145.4TCP system rules155.5TCP communication overview155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			5.3.3 TCP authenticity	
5.3.5TCP accountability			5.3.4 TCP reliability	
5.3.6TCP portability			5.3.5 TCP accountability	
5.4ICP system rules155.5TCP communication155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35		<b>F</b> 4	5.3.6 TCP portability	
5.51CP communication155.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex C (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35		5.4	TCP system rules	
5.5.1TCP communication overview155.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35		5.5	ICP communication	
5.5.2Secure envelope175.5.3TCP message package185.5.4TCPSPs' communication binding196Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			5.5.1 ICP communication overview	
5.5.3   TCP message package   16     5.5.4   TCPSPs' communication binding   19     6   Trusted communication evidence (TCE)   21     6.1   TCE generation   21     6.2   Evidential procedure   23     6.3   TCE custody   24     6.3.1   General   24     6.3.2   TCE Generation   24     6.3.3   Validation about TCE   25     6.3.4   Archiving of TCE   26     Annex A (informative) Trusted communication reference model   28     Annex B (informative) TCP main: quality and risk management   29     Annex C (informative) TCPSPs' communication binding (an example)   31     Bibliography   35			5.5.2 Secure envelope	1/
6   Trusted communication evidence (TCE)   21     6.1   TCE generation   21     6.2   Evidential procedure   23     6.3   TCE custody   24     6.3.1   General   24     6.3.2   TCE Generation   24     6.3.3   Validation about TCE   25     6.3.4   Archiving of TCE   26     Annex A (informative) Trusted communication reference model   28     Annex B (informative) TCP main: quality and risk management   29     Annex C (informative) TCPSPs' communication binding (an example)   31     Bibliography   35			5.5.5 TUP message package	10
6Trusted communication evidence (TCE)216.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative)Trusted communication reference model28Annex B (informative)TCP main: quality and risk management29Annex C (informative)TCPSPs' communication binding (an example)31Bibliography35			5.5.4 TCPSPS communication binding	19
6.1TCE generation216.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35	6	Trus	ted communication evidence (TCE)	
6.2Evidential procedure236.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35		6.1	TCE generation	
6.3TCE custody246.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35		6.2	Evidential procedure	
6.3.1General246.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35		6.3	TCE custody	
6.3.2TCE Generation246.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			6.3.1 General	
6.3.3Validation about TCE256.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			6.3.2 TCE Generation	
6.3.4Archiving of TCE26Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			6.3.3 Validation about TCE	
Annex A (informative) Trusted communication reference model28Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35			6.3.4 Archiving of TCE	
Annex B (informative) TCP main: quality and risk management29Annex C (informative) TCPSPs' communication binding (an example)31Bibliography35	Ann	<b>ex A</b> (in	formative) Trusted communication reference model	
Annex C (informative) TCPSPs' communication binding (an example)   31     Bibliography   35	Ann	ex B (in	formative) TCP main: quality and risk management	
Bibliography 35	Ann	ex C (in	formative) TCPSPs' communication binding (an example)	
	Bibl	iograpł	ıy	

# 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 <a href="https://www.iso.org/directives">www.iso.org/directives</a>).

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 <a href="https://www.iso.org/patents">www.iso.org/patents</a>).

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 <a href="https://www.iso.org/iso/foreword.html">www.iso.org/iso/foreword.html</a>.

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 <u>www.iso.org/members.html</u>.

# 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.

<text> 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 7<sup>th</sup> 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 <u>https://www.iso.org/obp</u>
- IEC Electropedia: available at <u>http://www.electropedia.org/</u>

#### 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