

1 RESTRICTED

2 **CEFACT/2013/ITXXX**
3 **July 18, 2013**

4
5
6
7
8
9
10
11
12
13
14 **UNITED NATIONS**
15 **CENTRE FOR TRADE FACILITATION AND ELECTRONIC BUSINESS**
16 **(UN/CEFACT)**

17
18
19
20
21
22
23
24 **INTERNATIONAL TRADE PROCEDURES DOMAIN GROUP**
25 **Trade and Transport Programme Development Area**

26
27
28
29
30
31 **Recommendation 14**

32
33 **Authentication of Trade Documents**

34
35
36
37
38
39
40
41
42
43
44
45
46
47 **SOURCE: Recommendation 14 Revision Project Team**
48 **ACTION: Finalized draft (for Public Review)**
49 **STATUS: Draft v1.0**

50 **Foreword**

51

52 **Introduction**

53 The exchange of accurate, complete and timely information is fundamental to the efficient
54 and effective conduct of domestic and international trade. Traditionally the exchange has been
55 conducted by the use of paper-based documents. Increasingly, electronic equivalents to paper
56 have improved the speed and efficiency of data exchange for trading partners, trade services
57 providers, government and other regulatory authorities and agencies.

58

59 A constant and continuing objective of the United Nations Centre for Trade Facilitation and
60 Electronic Business (UN/CEFACT) is the reduction of documents used in the supply chain
61 between business partners both domestic and international. Where removal is not possible
62 because of legal obligation, regulatory requirement or business need, UN/CEFACT has
63 pursued the objective that the document should NOT require a signature to convey the intent
64 of the party originating it or for the recipient to act on the information contained in it.

65

66 UN/CEFACT recognizes the aim of removing signature from all trade documents that remain
67 in the supply chain is probably unattainable. Some trade documents will of legal necessity
68 continue to require a signature. The requirements for a signature are tied to the use of paper
69 documents. The ever increasing use of electronic or other automatic means of data transfer
70 makes it desirable to find alternative authentication methods, some of which may eliminate
71 the need for a signature entirely and some which may provide the electronic equivalent of a
72 manual-ink signature. Since the first version of this Recommendation in 1979, a number of
73 alternative methods of authentication have appeared and will probably continue to appear in
74 the years ahead.

75

76 **Part ONE: Recommendation 14 On Authentication of Trade Documents**

77

78 **1. Scope**

79 This Recommendation seeks to encourage the use of electronic data transfer in international
80 trade by recommending that Governments review national and international requirements for
81 signatures on trade documents in order to eliminate the need for paper-based documents by
82 meeting the requirement for manual-ink signatures through authentication methods that can
83 be electronically transmitted.¹

84

85 Similarly, this Recommendation encourages the trading community and trade services
86 providers to examine business processes to identify where signatures (of any kind) may be
87 eliminated and for those processes where this is not possible, to pursue the electronic transfer
88 of trade data and the adoption of authentication methods other than the manual-ink signature.

89

90 **2. Use of International Standards**

91 The use of international standards can play a key role in larger acceptance of chosen solutions
92 and eventually, interoperability. In so far as possible, governments and private actors who
93 intend to electronically exchange data using an authentication method should try to make use
94 of existing international standards.

95

¹ For the transition from paper documents to electronic equivalents in the various functions of an international trade transaction, see Lauri Railas, *The Rise of the Lex Electronica and the International Sale of Goods, Facilitating Electronic Transactions Involving Documentary Credit Operations*, Forum Iuris, University of Helsinki, 2004, especially Chapter VIII.

96 This document is part of a package of recommendations on trade standardization and
97 facilitation (see Annex A3). There are many aspects to electronic data exchange, many of
98 which are the subject of several United Nations Economic Commission for Europe (UNECE)
99 current and future recommendations.

100
101 The legal codification work in electronic commerce and electronic signature, undertaken by
102 the United Nations Commission on International Trade Law (UNCITRAL) should be taken
103 into account and used whenever possible as a foundation for developing electronic
104 authentication legal infrastructure for both national and international transactions.

105 **3. Recommendation**

106 UN/CEFACT recommends that governments and those engaged in the international trade and
107 movement of goods:

- 108 • Actively consider the removal of the requirement for a signature (manual-ink or its
109 electronic equivalent) from trade documents except where essential for the function of
110 the document or the activity and refrain from requiring a signature in new rulings or
111 practices.
112

113
114 Further, the UN/CEFACT, recognizing the importance of authentication methods in electronic
115 exchange of trade-related documents, recommends that governments and those engaged in the
116 international trade and movement of goods:

- 117 • Consider the introduction of electronic methods to authenticate trade documents;
- 118 • Create a legal or contractual framework that permits and gives equal status to such
119 authentication methods.
120

121 In order to achieve this objective, UN/CEFACT recommends:

- 122 • A regular review of the documentation used for domestic and cross border trade by a
123 joint public and private sector working party (or sector-specific working parties). The
124 goal of the working party would be to eliminate the requirements for a manual-ink
125 signature and where this is not possible, replace the manual-ink signature with other
126 authentication methods.
127

128 **Part TWO: Guidelines for Implementing Recommendation 14**

129

130 **1. Introduction**

131 These Guidelines, which are complementary to UN/CEFACT Recommendation Number 14
132 on Authentication of Trade Documents, are designed to assist Governments and Trade in
133 identifying the function and use of signature. They provide an overview of the main issues
134 that should be addressed, some of the tools that are available and the steps to be taken when
135 moving towards electronic methods of authentication.

136

137 This Recommendation will be accompanied by two Annexes aimed at assisting Governments
138 and Trade to envision ways in which electronic methods of authentication have been put in
139 place or are currently implemented.

140

141 **2. Signature**

142 **2a. Definition of Signature**

143 The word “signature” in today’s vocabulary encompasses both manual-ink signature and its
144 electronic equivalent. The original 1979 version of this Recommendation makes no
145 distinction in the title because at that time, a signature was considered to always be manual-
146 ink. As such, this term requires further precision in the current Recommendation title and
147 throughout this document.

148

149 In its broadest sense, a signature (manual-ink or its electronic equivalent) creates a link
150 between a person (physical or legal) and the content (document, transaction, procedure, or
151 other). This link can be considered as having three inherent functions: an identification
152 function, an evidentiary function and an attribution function.²

153

154 In international business relations, one of the basic foundations is trust between the parties;
155 the requirements of a signature will, in many cases, most likely reflect that trust.

156

157 **2b. Functions of a Signature**

- 158
- 159 • The identification function of a signature confirms or allows the establishment of the
160 identity of that signatory; identification can include: the claimed/asserted identity of
161 the person, the veracity of the identity claims, the credentials of any verifying
162 organism, the proof of origin, the time and date, and any other aspect which identifies
the related persons or the content.
 - 163 • The evidentiary function of a signature will involve legal implications and can
164 include: integrity, consent, acknowledgement, and detection of any changes in the
165 document after it was signed. It can reflect any level of commitment which the act of
166 signing might have indicated.
 - 167 • The attribution function of a signature is the link between the signatory and the
168 document which is signed. This can include the authority granted within the role (i.e.

² These ideas of functions are developed in paragraph 7, page 5, UNCITRAL “Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods,” United Nations, Vienna 2009. Available as of March 2013 at

http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf.

See also "Review of Definitions of "Writing," "Signature" and "Document" employed in multinational conventions and agreements relating to international trade, submitted by the Legal Working Group (LWG), Revision of Document Trade/WP.4/R.1096 dated 22 July 1994; TRADE/CEFACT) Geneva, October 2001, ECE/TRADE/240."

169 within a company, within a government authority, within the market...) of the
170 signatory.

171
172 These three functions can be considered to be on variable levels. There can be more or less of
173 each of these functions inherent in any signature.

174 175 **2c. Methods of Authentication**

176 A signature or its functional equivalent is a common method of authentication and as such the
177 terms “to sign” and “to authenticate” are used as synonyms in these Guidelines.³

178
179 The usage or the requirement of a manual signature presents major problems for modern high-
180 technology data transfer in those instances where the data is transmitted from the country of
181 purchase to the country of (final) destination and where the manual signature must be
182 available at the clearance of the goods. National legislation and international conventions
183 should be changed wherever they impose a manual signature as a guarantee for the
184 authenticity of information transmitted in this way.

185 186 **3. Requirement for Signatures on Trade Documentation**

187 In general, there are various uses of a signature on trade documentation. When considering a
188 transaction from a manual-ink signature process to its electronic equivalent, it is necessary to
189 consider the context of the transaction itself.

190 191 **3a. Considering the Legal Context of the Transaction**

192 Generally, for business to business transactions, the legal requirements can be within the
193 framework of commercial law. The requirements or trade practices may be further developed
194 or defined by trade organizations for their members. Finally, many requirements within
195 transactions between two independent trading partners will be explicitly defined in bilateral or
196 multilateral agreements.

197
198 For transactions with government authorities or among government authorities, the legal
199 requirements are defined almost exclusively within the framework of public law.

200
201 There may be several layers of public and private law to be considered: at a federal level, at a
202 state level, at a ministerial level, at an agency level, at a regional level, at an international
203 level, etc. It may also be necessary to consider several types of public regulations:
204 commercial regulations, transport regulations, health regulations, customs regulations, etc.

205
206 Furthermore, a same document may be used by several agencies of a same government, or
207 even of different governments. This may happen for instance, in the framework of single
208 window facilities or coordinated border management. In these cases, the requirements of

³ Care should be taken when considering the terms presented here in Section 2 (signature, function of signature and authentication). There are often different understandings of these terms depending on the environment (legal or technical). There can be further differences based on the region of the world these terms are being used. In general, signature and authentication in an Information Technology (IT) environment often encompass some inherent functions which can vary from integrity, genuineness, proof, security, etc. Again, all of these terms can have differing interpretation based on environment and geography.

This Recommendation has been prepared to align itself with the works of UNCITRAL while remaining consistent with the use of these terms in other UNECE Trade Recommendations.

When reading or drafting any text on the subject, clear identification of which approach is being used, is recommended. For legislators who will probably use a legal definition, reference to UNCITRAL documents on the subject is recommended in order to clearly identify the legal use of these terms.

209 authentication will need to be aligned so as not to put into doubt the validity of the data which
210 is being communicated.

211
212 Legislation must not create stringent requirements which would put in doubt the validity and
213 enforceability of otherwise legitimate transactions.

214

215 **3b. Trade Documents**

216 Several interests can be affected by a chosen method of authentication; these include
217 commercial, transport, financial and official. Problems may arise in documents that cross
218 borders as they must be used in two different countries or regions. It should also be noted that
219 the information in some documents may be of interest to more parties than the original and
220 the final recipient of the documents.

221

222 Commercial documents can include the commercial invoice, certificate regarding quality and
223 quantity, shipping advice and, or notification and credit note. The main principle of
224 international trade law is that there is no formal requirement for a signature. Subject to an
225 exceptional requirement of signature in national law, documents required for the practical
226 performance of a contract need not therefore be signed.

227

228 Transport documents often involve a number of parties apart from the carrier themselves:
229 exporters, importers, financiers, insurers and authorities. The documents can include Export
230 Cargo Shipping Instruction, Bill of Lading, Sea and, or Airway Bill, Consignment Note and
231 Certificate of Shipment. Many of these documents are covered by international conventions
232 that impose internationally binding obligations and conditions and are often enforceable by
233 national laws and regulations. Some of these conventions still mandate a signed document to
234 perform a particular function in the transport, transit or logistics chain. However, many more
235 conventions have adopted a more modern, simpler approach by removing the requirement for
236 a manual signature and replacing it with an electronic equivalent or another method of
237 authentication.⁴ Consequently the domestic and international transport chains are
238 increasingly demonstrating the tendency that the requirement for a signature is not necessary.

239

240 Financial documents can include insurance policy or certificate, bank transfer, specific bank
241 documentary provisions of the credit or collection, and bills of exchange. The same
242 considerations would largely apply as with transport documents. Many of these documents
243 have already been replaced by automated processes that relate to relationships between the
244 financial institutions. Some financial documents, most notably bills of exchange are
245 negotiable instruments, where form and signature requirements are well established. However
246 this does not preclude actions to remove these requirements and replace them with more
247 modern, simpler methods or authentication.

248

249 Official documents can include customs export declarations, import entries, import
250 certificates, agricultural certificates, CITES (Convention for the International Trade in
251 Endangered Species) certificates, and other documents required to establish admissibility and
252 accountability. The acceptance and responsibility to meet official and regulatory demands
253 often occurs at import in the country of final destination. However, meeting these
254 requirements often has a direct bearing on action in the country of export before or at the time
255 of dispatch, or subsequently.

⁴ UNCITRAL has on-going work on this subject. See, among other references, the 47th Session Working Group at http://www.uncitral.org/uncitral/en/commission/working_groups/4Electronic_Commerce.html (as of 1 July 2013) and the draft model terms is A/CN.9/WG.IV/WP.122.

256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302

3c. Determining the Needs of Authentication In the Context of a Transaction

For transactions with government authorities, it is recommended that a joint public and private sector working party (or sector-specific working parties) be established in order to perform a regular review of the documentation used for domestic and cross border trade. The goal of the working party would be to eliminate the manual-ink signature whenever possible and either eliminate its necessity completely, if this is safe and reasonable in the context of the transaction, or replace it with other authentication methods. A list of considerations is proposed in Annex B.1.

For business to business transactions, the two parties can likewise study the needs of authentication in the context of individual transactions. The list of considerations proposed in Annex B.1 should also provide guidance in this context.

4. Use of Electronic Authentication Methods

The choice of other authentication methods will depend on the business process and a risk assessment of the needs of that process. A list of considerations when choosing an electronic authentication method is proposed in Annex B.1.

4a. Technology Neutrality

In so far as possible, legislation should remain technology neutral; it should not discriminate between forms of technology. Technological guidance, when provided, should be based on minimal requirements perhaps with examples, but with the possibility of responding to these requirements with other solutions which would be functionally equivalent.

4b. Levels of Reliability

As described above, depending on the relationship between the parties and the context of the legal environment, some processes may require more or less security. Not every transaction needs to be the highest level of security. Likewise, technological methods vary and may provide more or less security as required.

The chosen method of authentication should be “as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.”⁵

Efforts should be made to avoid creating electronic solutions which are more cumbersome or costly than the manual process. Technology can provide implementations with very high levels of reliability. Implementation choice should be in line with the level of reliability required by the process and existing legal constraints.

4c. Typologies of Electronic Authentication Methods

A number of alternative methods exist that can replace a manual-ink signature. Technology is constantly evolving. Illicit or fraudulent activity is also constantly evolving, finding ways to undermine the level of reliability that might be placed in some aspects of a given method. For this reason, technical standards and technical implementations are further discussed in Annex B.2 of this Recommendation in order to facilitate its updating to correspond to current best practices and standards.

⁵ Article 7.1, UNCITRAL “Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998” United Nations, New York, 1999, p.5-6. Available as of March 2013 at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.

303
304 Depending on risks, security needs, and other considerations, an authentication method used
305 alone ("single factor authentication") may suffice. In high-risk situations however, an
306 appropriate combination of authentication methods and other techniques may be needed
307 ("multi-factor authentication"). For example, a registration and verification process may be
308 based on an ID/Password for identification accompanied by a Virtual Private Network (VPN)
309 or other electronic method.

310 311 **4d. Electronic Signature**

312 Almost without exception, all of these methods can generally be referred to as an electronic
313 signature. An electronic signature can be defined as "data in electronic form in, affixed to or
314 logically associated with, a data message, which may be used to identify the signatory in
315 relation to the data message and to indicate the signatory's intention in respect of the
316 information contained in the data message."⁶

317
318 It should be noted that an electronic signature in this broad sense does not inherently call for a
319 specific form of technology. An electronic signature will serve the same functions as a
320 manual-ink signature, again on a sliding scale with more or less of each of these functions
321 (that is, identification, evidentiary and attribution).

322
323 An electronic signature should not be discriminated because of its origin. It should also not be
324 discriminated merely because it is an electronic authentication method. However, it may be
325 discriminated because of its intrinsic qualities.

326
327 A distinction should be made between "electronic signature" as it is used in this guideline and
328 relevant UNCITRAL texts on electronic commerce and "digital signature" which is addressed
329 in the Annex B of this Recommendation. For the sake of clarity, it is underlined that these two
330 terms are not interchangeable. The generic term, which makes no reference to any
331 technological choice, and used in UNCITRAL texts on electronic commerce, is "electronic
332 signature." "Digital signature," as discussed in UNCITRAL documents, implies that a
333 technological choice has been made (for solutions with asymmetrical encryption, Public Key
334 Infrastructure (PKI) signature technology being the main example).⁷ Regulators and those
335 drafting contracts or technical documents, should bear this distinction in mind and use the
336 term "electronic signature" unless they intend to imply such a technological choice has been
337 made.

338 339 **5. Aspects for Consideration of Electronic Authentication Methods**

340 These are some aspects that should be considered depending on the chosen methods of
341 authentication.

342 343 **5a. Use of Third Party Services**

⁶ Cf Article 2a of the UNCITRAL "Model Law on Electronic Signature with Guide to Enactment 2001," United Nations, New York 2002, page 1. Available as of March 2013 at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html. Note that the original definition in this 2002 document cites the "signatories' approval," Further UNCITRAL work has evolved towards the "signatories' intention."

⁷ Cf for example paragraph 21, page 15, UNCITRAL "Promoting Confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods," United Nations, Vienna 2009. Available as of March 2013 at http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf.

344 The parties may prefer or need to call upon a third party to perform any aspect of
345 transmission, archival, retrieval, verification, etc., involved in the authentication method. In
346 some cases, third party services are mandated or validated by a government authority (issuing
347 encryption keys, for example). In some cases, third party services offer options to trading
348 partners for full plug-and-play solutions, data compilation and transmission services,
349 enhancement of security, archiving/retrieval services, etc.

350

351 In a very general sense, authorization to use a third party service should be granted by either
352 trading partner. In this case, the third party service would be considered an ‘intended party’ /
353 ‘authorized party’ in the transaction process. Any limitations to this authorization or the
354 possibility to use a third party service should be clearly outlined in the appropriate legal text,
355 the bilateral agreement between trading partners or agreements with the third party services.

356

357 Where third party services are mandated or validated by a government authority, the
358 requirements to become mandated should be transparent and the process should be open to
359 all.

360

361 **5b. Security of Data**

362 Access to the data should be limited to the intended parties (authorized parties). This can in
363 part be determined by the legal responsibilities of the parties involved.

364

365 The requirements of the security of the data will correspond with the level of reliability
366 required by the transaction which should have been determined by a risk assessment
367 considering the process, the operational constraints, the legal constraints and the relationship
368 of trust between the parties. If a trusted third party is acting within the process, they should
369 ensure this same level of reliability. Depending on the determined level of reliability, parties’
370 interests in the event of litigation should be protected.

371

372 Depending on the level of reliability, security of the data may encompass ensuring protection
373 and ensuring that data is not deleted or destroyed.

374

375 **5c. Transmission of Data**

376 The aspects of the actual transmission of data will depend on the electronic method chosen.
377 These are presented in the Annex B of this Recommendation.

378

379 For private business to business exchanges, the two parties should explicitly agree on the
380 method of communication and the method of authentication. They should consider the level
381 of reliability required when establishing this agreement. This could, for example, be part of an
382 Interchange Agreement between the two parties as per the model of UN/CEFACT
383 Recommendation 26.

384

385 Depending on the level of reliability, an audit trail may be necessary. In some cases it may be
386 useful or legally necessary to obtain confirmation of transmission / confirmation of receipt,
387 ensuring the order of messages, time stamp, the various headers, etc. This may be required
388 under certain trading partner agreements or in a particular legal context.⁸

389

390 **5d. Archiving / Retrieval**

⁸ In this regard, reference may be made to article 15 of the UNCITRAL Model Law on Electronic Commerce and article 10 of the Electronic Communication Convention which provides rules on the time and place of dispatch and receipt of data messages.

391 In most cases, trade documents will need to be archived either for later use for other
392 processes, for a trace of the operations, etc., or in order to respond to legal obligations or
393 regulatory requirements (for example the legal requirements to archive electronic invoices or
394 customs declarations). When considering the archiving of trade documents, the party should
395 consider the archiving period, archiving place, and access control. Authentication method for
396 archiving documents could be very different depending on long-term archiving or short-term
397 archiving. Documents archived for long periods may require special attention, as existing
398 authentication methods commonly weaken or even become obsolete over time due to new
399 technologies. Governments or bilateral agreements may want to foresee migration from one
400 technology to another during archiving.

401
402 Archiving methods are expected to correspond to at least an equivalent level of reliability as
403 the authentication/signature method used. The method of archiving should be auditable; in
404 other words, it must be possible to check its reliability to see whether it works or not, to check
405 the correctness of retrieved data and its readability (format used), and to verify that it
406 encompasses the functional aspects of an authentication which is being accepted between the
407 parties and authorities.

408
409 The trading partners may wish to call upon a third party service to assist in archival and
410 retrieval of the data; this may be dependent on many factors including technological
411 capabilities and costs. In this case, the third party services should take into consideration the
412 above points. Third party solutions may also have the possibility to issue a certificate with
413 legal effect proving that an authorized party retrieved the data and when it was retrieved, if
414 the level of reliability calls for such provisions.⁹

415 416 **6. Recommendation Review Process**

417 The present Recommendation is divided into the Recommendation text, Guidelines and
418 Annexes (which include Repositories). It is suggested that the Annexes and Repositories are
419 updated every three to five years. This will entail contacting each initial contributor to verify
420 that the information is still pertinent / up-to-date (absence of a response should result in the
421 elimination of the submission from the Annex). Following the response from the contributor,
422 the information in the Annex should be confirmed, revised or eliminated as the case may be.
423 This will also be an opportunity to request new submissions for the Annexes and integrating
424 any other contributions.

425
426 Once all of the Annexes and Repositories have been updated, it is suggested that the content
427 of the Recommendation and its Guidelines be verified against the revised Annexes. If there
428 are no (or very minor) modifications, it may be best not to update the Recommendation in the
429 interest of trying to keep a stable version. If there are elements from the Annexes and
430 Repositories which contradict or render the Recommendation text obsolete / erroneous the
431 Recommendation should be modified.

432
433 Similarly, if Governments or Trade bring substantive concerns to light as to the pertinence of
434 the text of the Recommendation, this should be considered for purposes of text revision even
435 outside of the updating periods.

436 437 **7. Options Other Than a Manual-Ink Signature**

⁹ In this context, reference may be made to article 10 of the UNCITRAL Model Law on Electronic Commerce which provides a rule on retention of data messages.

438 This chapter aims to bring further precision to the three main recommendations of this
439 document.

440

441 **7a. Removal of Manual-Ink Signatures and Their Electronic Equivalent When Possible**

442 It is recommended that Governments and all organizations concerned with the facilitation of
443 international trade procedures examine current trade documents to identify those where
444 manual-ink signatures and their electronic equivalent could safely be eliminated and to mount
445 an extensive program of education and training in order to introduce the necessary changes in
446 commercial practices.

447

448 This removal of the requirements for a signature should be studied on a case-by-case basis for
449 each given commercial document. Where signature is not essential for the function of the
450 document or the transaction, then it is recommended that these requirements be removed.

451

452 Furthermore, when creating new trading environments or documents, it is recommended to
453 naturally refrain from introducing requirements for signatures in new regulations, rulings,
454 contracts or practices.

455

456 **7b. Enabling Electronic Methods of Replacing a Manual-Ink Signature**

457 It is recommended to Governments and international organizations responsible for relevant
458 intergovernmental agreements to study national and international texts which embody
459 requirements for signature on documents needed in international trade and to give
460 consideration to amending such provisions, where necessary, so that the information which
461 the documents contain may be prepared and transmitted by electronic means.

462

463 Amending the relevant provisions in every legal text where a signature is mentioned is not
464 feasible given the very high number of occurrences. In order to resolve this at the national
465 level, it is recommended to adopt legislation establishing functional equivalence between
466 electronic and paper-based signatures such as that based on the UNCITRAL Model Law on
467 Electronic Commerce and on the UNCITRAL Model Law on Electronic Signatures. This
468 blanket provision would reinterpret any reference to signature or authentication as meaning
469 the possibility to allow for their functional electronic equivalent. At the international level, the
470 same result may be achieved with the adoption of the United Nations Convention on the Use
471 of Electronic Communications in International Contracts, 2005 (article 9(3)).¹⁰ Since the
472 Convention applies to international transactions only, it is also recommended to create a
473 concurrent legal text for domestic transactions with such a blanket provision which would
474 reinterpret any reference to signature or authentication as encompassing their functional
475 electronic equivalent.

476

477 It is suggested that the paper-based process be identified and that this process be detailed step-
478 by-step. Risk-assessment should be a guiding principle, considering the context of the
479 transaction/service, the legal constraints, the operational constraints, etc. Parties should be
480 permitted and encouraged to fulfill functional requirements of a manual-ink signature by
481 using other methods.

482

483 **7c. Creation of Legal Framework**

¹⁰ “United Nations Convention on the use of Electronic Communications in International Contracts” (Electronic Communications Convention [ECC]) United Nations, New York, 2007. In force since March 2013. Available as of March 2013 at: http://www.uncitral.org/pdf/english/texts/electcom/06-57452_Ebook.pdf

484 Examples of legally enabling environments are provided in Annex A. The operational
485 capability of replacing a manual-ink signature by an electronic method must be accompanied
486 by appropriate legislation which gives equal status to those authentication methods. This legal
487 framework should foresee the acceptability in court of alternative transmission methods and
488 archiving processes. Two main aspects may need to be addressed either jointly or separately:
489 the legal framework for private-sector operations and the legal framework for operations
490 between the private sector and government agencies.

491
492 Concerning operations between private businesses and between business and consumers,
493 governments should undertake a study (including e-Commerce legal benchmarking and “gap
494 analysis” studies) to determine an appropriate set of measures that may need to be taken to
495 address legal issues related to authentication of national and cross-border exchange of trade
496 data.

497
498 Concerning operations between business and government agencies, the government, at the
499 highest level, must first provide the legislative mandate for agencies to provide the option for
500 electronic maintenance, submission, or disclosure of information, when practicable as a
501 substitute for paper. As part of this mandate, the Government should, in consultation with
502 other agencies and the private sector, develop practical guidance on the legal considerations
503 related to agency use of electronic filing and record keeping so that the agency can in return,
504 make the appropriate assessment for its mission. Consideration should be given by the agency
505 on how to design the process to protect the agency’s legal rights and how best to minimize
506 legal risks to the agency.

507
508 Government should, when possible, provide guidance to the private community on this issue.
509 Any guidance provided by the Government and/or the specific agency should also take into
510 consideration current legal requirements pertaining to the use, storage and disclosure of
511 information, and its use as evidence in courts or administrative bodies.

512
513 The legislative frameworks should be reviewed regularly in order to correspond to actual
514 business practices. Public law should aim, whenever possible, to align with current way of
515 doing business and with current best practices and standards.
516

517 **Annex A1 – Legally Enabling Environment**

518

519 **Recommended Checklist for Government Agencies When Reviewing Their Legal**
520 **Environment**

521

522 ✓ Compliance with applicable laws and regulations?

523 ✓ Compliance under confidentiality laws?

524 ✓ Comprehensive plan to address all issues raised by moving to an electronic
525 system?

526 ✓ Consultation with impacted parties, including other relevant offices and agencies?

527 ✓ Is any information used in the process required by law or regulation to be in a
528 particular form, paper or otherwise? If part of the process is paper, how will this
529 be satisfied?

530 ✓ Is there a legal requirement or an agency need to maintain the information? And if
531 so, for how long?

532 ✓ Is the information of importance to national security, public health or safety, public
533 welfare, the protection of the environment, or other important public purposes?

534 ✓ Is there impact to the public if this information is not available?

535 ✓ What is the importance of the information to the agency's mission/ programs?

536 ✓ Is there a revenue impact to the agency?

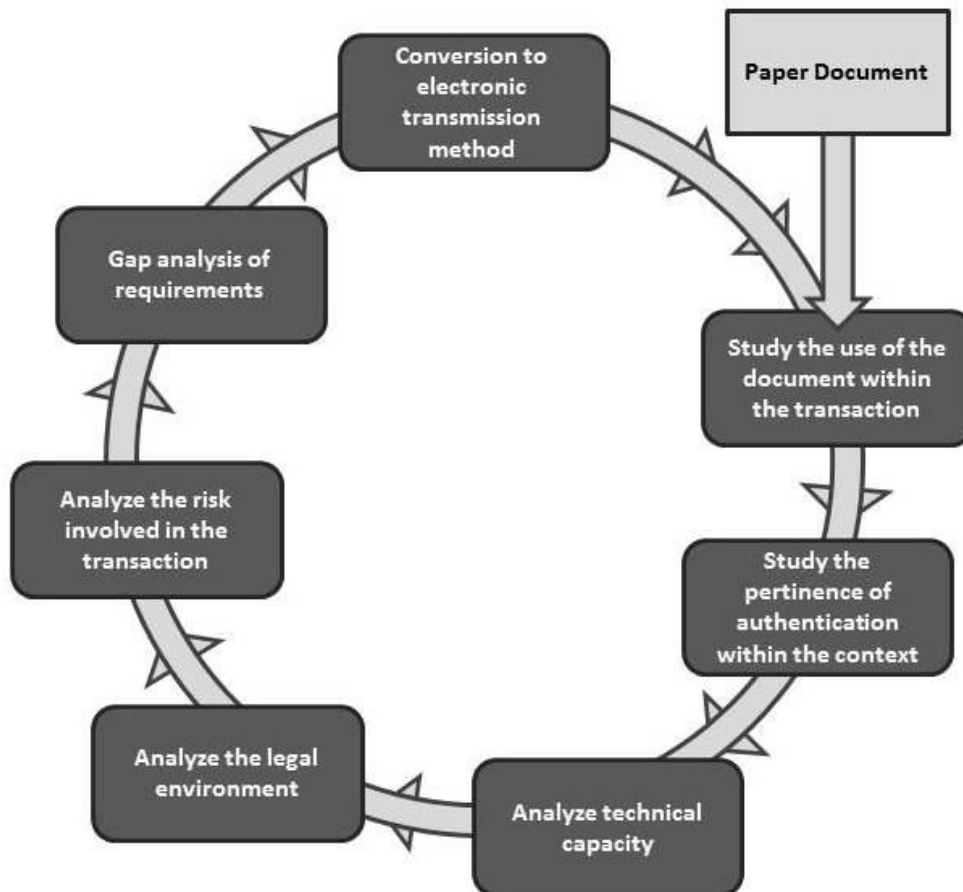
537 ✓ Might the information be needed for use in criminal proceedings or other legal
538 proceedings?

539

540 **Annex A2 – Virtuous Circle for the Review of Trade Documents**

541
542 To achieve the objective of removing the requirement for a signature on trade documents, or
543 where that is not immediately possible, to consider other methods of authentication,
544 Recommendation 14 recommends a regular review of the documents used in domestic and
545 cross border trade. The review would be conducted by a joint public and private sector
546 working party to ensure that the regulatory and official requirements and the business needs
547 of the trading community are fully considered in an open, transparent and inclusive way.

548
549 The suggested methodology of the working party is shown in the figure below:
550



551
552
553 **Figure 1**

554
555 The ‘virtuous circle’ diagram envisages a rolling programme of review for all documents used
556 in domestic and international trade conducted every three to five years. For ease of conducting
557 the programme and utilizing the expertise of the participants in the working party, the
558 documents should be divided into specific functional groups, for example Commercial,
559 Transport, Financial (including international payments) and Official. The suggested divisions
560 are indicative and not exhaustive.

561
562 A schedule or calendar for the document groups should be agreed by an oversight or
563 supervisory committee to ensure consistency of methodology and outputs from each group.
564 Adopting this approach should make the review programme manageable, efficient and

565 effective. Equally a structured programme should reduce the time and burdens on participants
566 of the individual review groups.

567

568 The outcome from the rolling programme would be an action plan to remove the requirement
569 for a signature from a significant number of trade documents. Where this is not immediately
570 possible the action plan should offer imaginative and innovative ways of replacement by other
571 authentication methods. In this respect the members of the review groups should embrace the
572 concept of simpler, easier trade processes through radical yet well informed and considered
573 solutions.

574

575 If, or when adopting the concept of a Virtuous Circle review program, the working party
576 would need to consider certain pre-requisites to ensure the review is successful. First and
577 foremost would be the technical capacity of both government and the business community to
578 implement any proposed action plan. The working party would need to ascertain the ability of
579 government to receive, share (among authorities and regulatory agencies), store and retrieve
580 data, and be able to accept and process other forms of authentication.

581

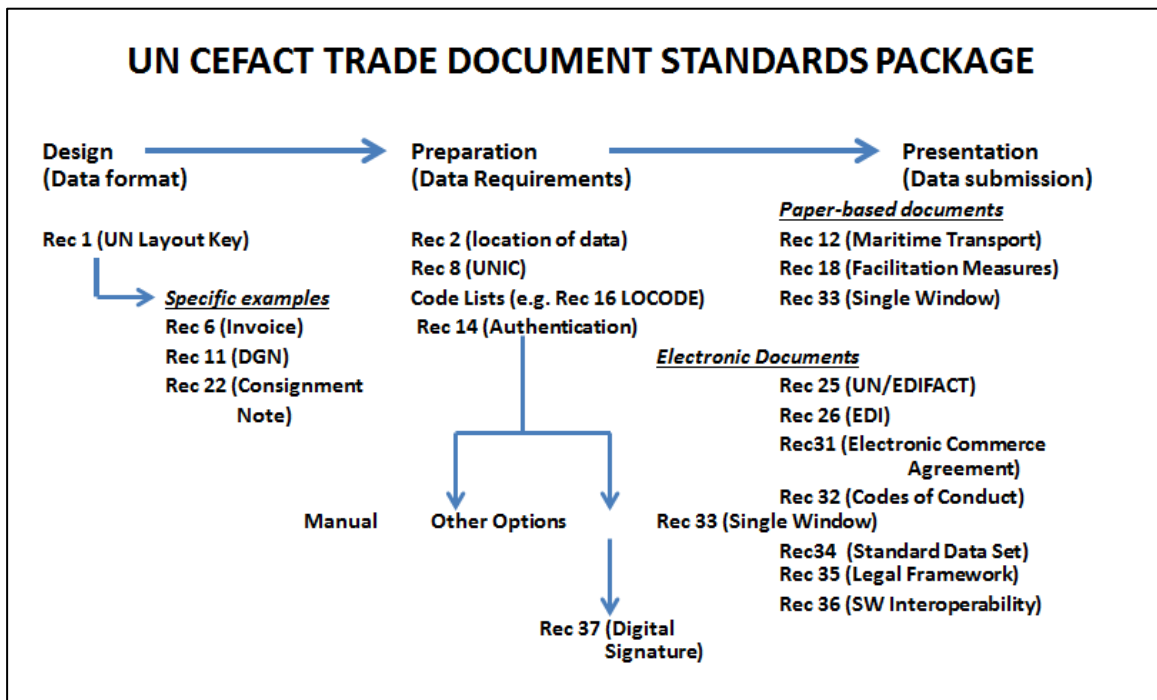
582 For the business community, especially the small and medium size enterprise sector, the
583 working party would need to determine traders have the ability to generate, receive and
584 process standard electronic data messages. Business should also demonstrate the ability to
585 maintain the electronic information for any government audit based controls using company
586 systems and commercial records. Equally important for the assessment of capacity is to
587 ensure business law will allow other forms of authentication other than signature to commit
588 the trading partners to the performance of the contracts in the trade transaction.

589

590 **Annex A3 – Trade Documents Standards Package**

591

592 UN/CEFACT provides a suite of products that offer recommendations, guidance, advice and
 593 good practices for the design, preparation and presentation (including electronic submission)
 594 of trade documents used in domestic and cross-border trade. Recommendation 14 is one of
 595 the instruments in this suite of products and the diagram below, figure 2, gives a graphical
 596 representation of its related position in the integrated package of standards for trade
 597 documents.
 598



599
600

Figure 2

601 **Annex B1 – Technical Implementations.**

602

603 **Checklist of Considerations to Determine the Needs of Authentication in the Context of**
604 **a Given Transaction**

605

606 The following key points should be taken into consideration when determining the needs of
607 authentication. This list should be applicable to transactions with government authorities as
608 well as business to business transactions.

609

- 610 • Context considerations
 - 611 ✓ Is a signature required at all to authenticate the trade document?
 - 612 ✓ Is an electronic transmission of the document suitable?
 - 613 ✓ Kind of transaction
 - 614 ✓ Volume (number of individual) of transactions
 - 615 ✓ Value of the transaction
 - 616 ✓ Number of signatories per individual transaction
 - 617 ✓ Frequency at which the trade transactions take place
 - 618 ✓ Nature of the trade activity (who are the parties, the sector of activity)
 - 619 ✓ Cost and benefits
 - 620 ✓ Compliance with trade customs and practice
- 621 • Technological considerations
 - 622 ✓ System and equipment capabilities and their possible interaction
(hardware/software)
 - 623 ✓ When using an intermediary, the authentication procedures made available and
624 set forth by them (audit procedure?)
 - 625 ✓ What are the potential threats / risks / vulnerabilities to attacks?
 - 626 ✓ What are the strengths of each alternative authentication method?
 - 627 ✓ Compatibility issues of authentication methods
 - 628 ✓ Analysis of existing technology and usability of that technology for purposes
629 of data retention and/or future access
- 630 • Legal considerations
 - 631 ✓ Legal context (national [local, federal...], regional, international, sectorial,
632 jurisprudence, private law... as described above in point 3a)
 - 633 ✓ Adherence to the UNCITRAL Model Law on Electronic Commerce or
634 Electronic Signature which enable mutual recognition of authentication
635 methods
 - 636 ✓ International agreements / bilateral or multilateral mutual recognitions (for
637 example recognition of standards, financial arrangements, interoperability
638 issues, etc.)
 - 639 ✓ Awareness of legal concerns and/or regulatory restrictions in each trading
640 parties' environment
 - 641 ✓ Does the transaction require legal validity or is the authentication merely for
642 enhancing security?
 - 643 ✓ The existence of insurance coverage mechanisms against unauthorized
644 communications
- 645 • Relationship considerations
 - 646 ✓ Determination of the level of protection needed and the potential of risk of
647 liability for the agency / trading party
 - 648 ✓ Importance and the value of the information contained in the electronic
649 communication

- 650 ✓ Degree of acceptance or non-acceptance of the method of identification in the
- 651 relevant industry or field both at the time the method was agreed upon and the
- 652 time when the electronic communication was communicated
- 653 ✓ Relationship between the trading parties (trust, etc.)
- 654

655 **Annex B2 – Typologies of Electronic Equivalents to a Manual-Ink**
656 **Signature**

657
658 The different typologies of electronic equivalents to a manual-ink signature can include (this
659 is a non-exhaustive list, presented alphabetically in order to underline that there is no
660 promotion intended in any of these methods):
661

- 662 • Biometric methods
 - 663 ○ “A biometric is a measurement used to identify an individual through his or
 - 664 her intrinsic physical or behavioural traits. Traits that may be used for
 - 665 recognition in biometrics include DNA; fingerprints; iris, retina, hand or facial
 - 666 geometry; facial thermogram; ear shape; voice; body odour; blood vessel
 - 667 patterns; handwriting; gait; and typing patterns.” (UNICTRAL Promoting
 - 668 Confidence op.cit. §53).
 - 669 ○ The biometric measurement may be unique, but there may be other forms of
 - 670 system challenges such as ensuring that a given fingerprint (for example)
 - 671 belongs to a specific person.
- 672 • Clickable “OK” or “I accept” boxes
 - 673 ○ Clicking an “OK” or “I accept” box.
 - 674 ○ This will often be coupled with another identification process such as payment
 - 675 by a credit card (for payment) or an ID/Password. Even accepting a license
 - 676 with an “I accept” box will be followed by installing software (for example).
- 677 • Communication network
 - 678 ○ Identification by means of participating in a network. This can be within a
 - 679 larger multi-partite network (such as ODETTE in the automobile industry or
 - 680 SWIFT). This can also be point to point (such as a Virtual Private Network –
 - 681 VPN between two points of access)
 - 682 ○ This is often accompanied by another typology such as ID/Password.
- 683 • Devices (authentication with a mobile phone, for example)
 - 684 ○ Identification of the device using a technology such as text messages
 - 685 (receiving a validation code or sending a message when crossing the border).
 - 686 ○ The individual will need to be associated in some way to the device.
- 687 • Digital signatures
 - 688 ○ “Digital signature” is a name for technological applications using asymmetric
 - 689 cryptography, also referred to as public key encryption systems that ensure the
 - 690 authenticity of electronic messages and guarantee the integrity of the contents
 - 691 of these messages. The digital signature has many different appearances, such
 - 692 as fail stop digital signatures, blind signatures and undeniable digital
 - 693 signatures.
 - 694 ○ One consideration will be building the infrastructure to put in place and
 - 695 maintain the certification process.
- 696 • ID/Password
 - 697 ○ Passwords and codes are used both for controlling access to information or
 - 698 services and for “signing” electronic communications. In practice, the latter
 - 699 use is less frequent than the former because of the risk of compromising the
 - 700 code if it is transmitted in non-encrypted messages. Passwords and codes are
 - 701 however the most widely used method of “authentication” for purposes of
 - 702 access control and identity verification in a broad range of transactions,
 - 703 including most Internet banking transactions, cash withdrawals at automated

- 704 teller machines and consumer credit card transactions. (UNCITRAL
705 Confidence op.cit. §63)
- 706 • Image of a signatures
 - 707 ○ A manual signature which is scanned or sent via facsimile. It can be an entire
 - 708 document that has been manually signed and which is scanned / faxed. This
 - 709 can also be an image of a signature or a scanned signature which is then
 - 710 attached to the document afterwards.
 - 711 • PGP (Pretty Good Privacy)
 - 712 ○ "Pretty Good Privacy" (PGP) is a software to protect information based in two
 - 713 keys. The first one is a public-key cryptography to encrypt the information
 - 714 which is collected ignoring any personal identification. The second one is the
 - 715 decrypt key, which is a private code only known by the owner to recover the
 - 716 encrypted information.
 - 717 • Seals (company seal)
 - 718 ○ A digital signature which applies to a company as opposed to an individual.
 - 719 • Signatures on pads
 - 720 ○ Manually signing a tactical screen device.
 - 721 • Signature on file
 - 722 ○ Signing an agreement with a partner which (for example a travel agency)
 - 723 allows for the ability to telephone or email the partner to purchase
 - 724 products/services with the method of payment that they have on file.
 - 725 • "Something I know"
 - 726 ○ Verification of identity by responding to a question or providing information
 - 727 that only the individual would know.
 - 728 • Structural agreement enabling electronic data exchange with no authentication
 - 729 ○ Signing a one-time paper contract which enables electronic data exchange
 - 730 (IATA eAWB).
 - 731 • Third-party validation
 - 732 ○ An example includes identification of the issuing party of a document which is
 - 733 validated by a third party.
 - 734 • Typed signatures
 - 735 ○ Typing in the issuing party's name at the end of a document – an email for
 - 736 example (this is often checked within the context of the transaction – in this
 - 737 example, it can be counter-checked by the sender of the email).
 - 738

739 **Repository A – Legally Enabling Environment**

740

741 Submissions from the following countries:

742

743 • CH – Switzerland (State Secretariat for Economic Affairs – SECO)

744 • IN – India (National Information Center – NIC)

745 • IT – Italy (Italian Trade Commission – ICE)

746 • JP – Japan (Japan Association for Simplification of International Trade Procedures –
747 JASTPRO)

748 • KR – Republic of Korea (National IT Industry Promotional Agency – NIPA)

749 • TR – Turkey (Ministry of Customs & Trade – Department of e-customs)

750 • US – United States of America (Customs and Border Protection – CBP)

751

Switzerland

752

753

	BUSINESS / TRADE CONTEXT (VERY BRIEF)
<i>Please describe the business / trade context / need that was being addressed when you decided to move from physical to electronic signature. Why was this being put in place? What specific issues were being addressed?</i>	
<i>What types of trade documents were involved – be specific/ authenticated?</i>	Certificates of origin, special permits/Licenses/Certificates and Authorizations (e.g. weapons, narcotics or Kimberly certificates)
<i>Are there trade documents which do not legally require a signature?</i>	All except the above
	LEGAL CONTEXT
<i>Type of legal system</i>	International Agreements, Constitution, Customs Law/Acts, Ordinances
<i>What is the fastest that a legally enabling environment can be created?</i>	<p>Customs Law/Acts: 2 – 2.5 years (depending on the agenda of the parliament). Proposal made by customs (in coordination with the other involved departments), transferred to the 2 chambers of parliament, where it will be dis-cussed separately until an agreement has been reached (several hearings are possible). Depending on the content of the proposal a subsequent public vote can be mandatory.</p> <p>International Agreements: 1 - 3 years, depending on the negotiations. Similar procedure as above.</p> <p>Ordinances: approx. 1 year, depending on the responsible body</p>
<i>Environment for adding/amending laws</i>	A change to an existing law is faster than creating a new one (due to the smaller size) but the procedure is the same
	CONSULTATION / DEVELOPMENT (TRANSITION TO ELECTRONIC ENVIRONMENT)
<i>What considerations needed</i>	1. Do we still want/need document “xy” ? Yes/no?

<p><i>to be addressed before passing any laws creating the legally enabling environment?</i></p>	<ol style="list-style-type: none"> 2. If yes: Do we want/need this document “xy” in electronic form? Yes/no? 3. If yes: Is there already a legal provision in place allowing for this document “xy” to be presented electronically? Yes/no? 4. If yes: Is it sufficient (no further steps needed) or has it to be amended (amendment needed)? 5. If no: A legal environment allowing for this document “xy” to be presented electronically has to be created.
<p><i>How was the private sector involved in the process (public outreach, commentary period, etc.)?</i></p>	<p>As they have to bear the major part of the costs, they were involved from the beginning (in creating the legal base and the procedure). Regular information and consultations took place. Their input has been taken into account wherever possible and feasible. Together with them the procedures have been put in place (e.g. sending of the e-documents or giving access to their systems), deadlines have been fixed and the different implementation speed of the diverse companies has been taken into account.</p>
<p><i>Were there any unexpected obstacles or complications that needed to be addressed?</i></p>	<p>Some specialties (few use/limited to small geographic spaces) for specific situations were not suitable to be handled electronically (cost/benefit for customs and trade).</p>
	<p>DETAILS OF SOLUTION (REMOVING MANUAL SIGNATURE LEGAL ENVIRONMENT)</p>
<p><i>Please briefly note current laws and their role in removing manual signature / enabling electronic exchange of trade-related documents.</i></p>	<p>http://www.ezv.admin.ch/dokumentation/00474/02202/index.html?lang=de (only available in our official languages DE, FR and IT).</p> <p>Art. 28 customs law (ZG) - possibilities of declaration (written, oral, electronic, etc.)</p> <p>Art. 84, 92, 96, 97, 105, 125, 184 ordinance (ZV) - procedure of declaration</p> <p>Art. 3, 6, 6a, 8, 20c ff., 24 customs ordinance (ZV-EZV) - detailed procedure of declaration</p>
	<p>PRACTICAL EXPERIENCE IN USE OF THIS LEGAL ENVIRONMENT</p>
<p><i>Resulting implementation in public sector (relating to trans-boundary trade)</i></p>	<p>Changing towards electronic systems have been made in order to be able to keep up with the growing amount of trans-boundary traffic in connection with reduced staff (more efficient handling).</p> <p>Customs is responsible for all trans-boundary trade (representing the other concerned departments).</p>

	See below.
	CONTACT DETAILS

754

755 **Typologies of electronic methods**756 Generally the authentication by Swiss customs always consists of a combination of the
757 following different typologies of electronic methods:

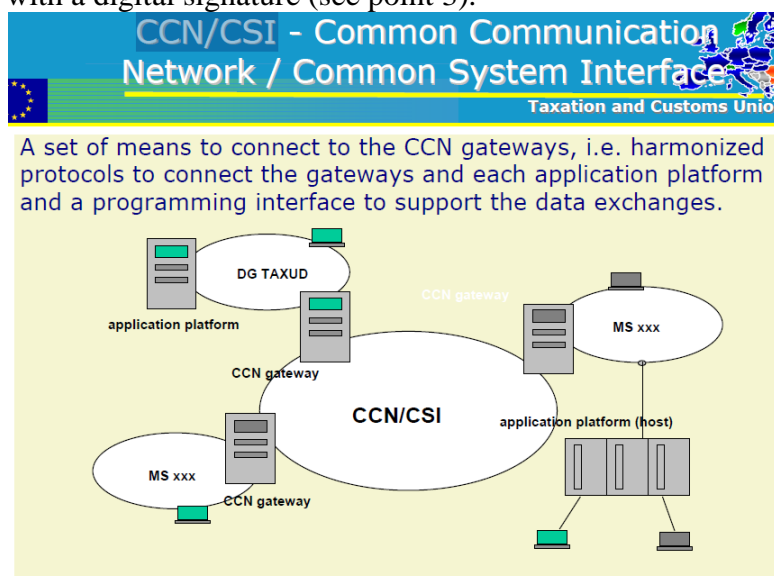
758 1. Communication channel (for example VPN)

759 a. Import/Export

760 The e-dec Service enables electronic filing of export or import, as well as the
761 acquisition of export customs declarations through an declarant. The service returns a
762 customs response including the associated PDF documents. Our service offers various
763 communication functionalities (Web service or Email). The two communication
764 channels can be used alternatively. The difference is technical: the Web service is a
765 synchronous service, the mail service is asynchronous. Both channels can only be used
766 with a digital signature (see point 3).

767 b. Transit

768 For the transit our external clients send the transit declaration via e-mail (SMTP).
769 This channel between the external clients and the Swiss customs administration can
770 only be used with a digital signature (see point 3).



A set of means to connect to the CCN gateways, i.e. harmonized protocols to connect the gateways and each application platform and a programming interface to support the data exchanges.

771

772 The channel between the customs administrations is secured (CCN/CSI).

773

774 2. Devices (authentication with a Smartphone, for example)

775 The employees of the Swiss customs administration use this device for the authentication
776 in conjunction with the UPN (User Principal Names). As an alternative to the
777 authentication via SMS, it is possible to authenticate via a Smartcard (with token; see point
778 6) as well.

779

780 3. Digital signatures (encryption, PKI)

781 a. Encryption: E-dec produces encrypted/signed mails using the IAIK-JCE Toolkit
782 (<http://jce.iaik.tugraz.at/products/01%5Fjce/>). The distribution of OpenSSL 0.9. 8i for

783 Windows can be performed the following steps (<http://www.openssl.org/>). For
 784 Registration & verification (see Point 5)

- 785 b. PKI: The following certificates are required:
- 786 i. Private certificate
 - 787 ii. Public certificate for e-dec for the corresponding environment (test or production)
- 788 Decryption and signature verification with the OpenSSL Toolkit

789 References:

Certificate Management with OpenSSL	http://gagravarr.org/writing/openssl-certs/general.shtml
OpenSSL Online Dokumentation	http://openssl.org/docs/
OpenSSL SMIME	http://openssl.org/docs/apps/smime.html
OpenSSL for Windows	http://www.slproweb.com/products/Win32OpenSSL.html

790 4. ID/Password

791 Employees of the Swiss customs administration use the UPN (User Principal Names) with
 792 password. Based on this, the customs officer accepts the declaration (hand- written
 793 signature is not used anymore).

794 5. Registration & verification process

795 To receive a PKI certificate, it is necessary to undertake a registration & verification
 796 process (manual procedure)

797 6. Tokens

798 The use of Smart Tokens (Smartcard, iKey) supplied by our IT provider assumes an
 799 appropriate Token Client. The Token is used for the smartcard (see point 2)

800

India

801

802

	BUSINESS / TRADE CONTEXT (VERY BRIEF)
<i>Please describe the business / trade context / need that was being addressed when you decided to move from physical to electronic signature. Why was this being put in place? What specific issues were being addressed?</i>	
<i>What types of trade documents were involved – be specific/ authenticated?</i>	
<i>Are there trade documents which do not legally require a signature?</i>	None. Signature is mandatory. There is no such initiation for removing signature so far
	LEGAL CONTEXT
<i>Type of legal system</i>	Information Technology Act, Digital/ Electronic signature
<i>What is the fastest that a legally enabling environment can be created?</i>	At present Digital Signatures are legally valid. Act also provides flexibility to add new electronic signature schemes. Such signatures Schemes should be notified in the second schedule. Ministry is authorized introduce new type of electronic signatures. The process of introduction of any new type signature may take 3-6 months.
<i>Environment for adding/amending laws</i>	The act empowers ministry to create new rules for authentication and introduction of new type of electronic signatures. ...? Parliament approval is not required however it is to be placed on the table of parliament for information.
	CONSULTATION / DEVELOPMENT (TRANSITION TO ELECTRONIC ENVIRONMENT)
<i>What considerations needed to be addressed before passing any laws creating the legally enabling environment?</i>	Electronic signature law exists. The current law states the electronic signature or electronic authentication technique should be considered reliable; and need to be specified in the Second Schedule. The reliability includes <ol style="list-style-type: none"> 1) signature linked to signatory and to no other person, 2) The signature creation data should be under the control of signatory

	<p>3) mechanism to detect the alteration to signature and signed data</p> <p>Legal recognition of electronic signature is based on the authentication by affixing the signature. The matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government</p>
<i>How was the private sector involved in the process (public outreach, commentary period, etc.)?</i>	Public can participate in the public review process.
<i>Were there any unexpected obstacles or complications that needed to be addressed?</i>	The reliability signature is to be examined before legal recognition.
	DETAILS OF SOLUTION (REMOVING MANUAL SIGNATURE LEGAL ENVIRONMENT)
<i>Please briefly note current laws and their role in removing manual signature / enabling electronic exchange of trade-related documents.</i>	
	PRACTICAL EXPERIENCE IN USE OF THIS LEGAL ENVIRONMENT
<i>Resulting implementation in public sector (relating to trans-boundary trade)</i>	At present digital signature is the only valid signature and for trans boundary trade, a cross certification is required.
	CONTACT DETAILS

Italy

804

805

	BUSINESS / TRADE CONTEXT (VERY BRIEF)
<i>Please describe the business / trade context / need that was being addressed when you decided to move from physical to electronic signature. Why was this being put in place? What specific issues were being addressed?</i>	Business simplification and facilitation, faster and easier data/documents exchange
<i>What types of trade documents were involved – be specific/ authenticated?</i>	In general, the digitalization process has progressively involved all trade and mandatory documents in Italy
<i>Are there trade documents which do not legally require a signature?</i>	As a general rule, all trade documents must be signed
	LEGAL CONTEXT
<i>Type of legal system</i>	Civil law
<i>What is the fastest that a legally enabling environment can be created?</i>	The Decree law concerning matters related to priority and national urgency (according to decisions of the Council of Ministers) is the fastest normative act in the Italian law system: it is approved by the Council and must be confirmed by a related law approved by the Parliament within 60 days. If not followed by such law, the Decree law expires. In principle, Decree laws may be used also for matters such as the creation of legally enabling environments, provided that they have the above mentioned priority and urgency requirements.
<i>Environment for adding/amending laws</i>	In general, There are several ways to promote a law in Italy. In particular, according to Italian relevant legal experience, for new or amended laws concerning the specific matters dealt with in this Annex A, either: <ul style="list-style-type: none"> • The Parliament mandates the Government to issue a Legislative Decree, setting specific guidelines and deadlines. The Government is therefore asked to comply accordingly. <p>Or</p>

	<ul style="list-style-type: none"> The Government or any member of the Parliament is entitled to issue a law proposal related to such matters; regular bicameral parliamentary procedures apply to these cases.
	CONSULTATION / DEVELOPMENT (TRANSITION TO ELECTRONIC ENVIRONMENT)
<i>What considerations needed to be addressed before passing any laws creating the legally enabling environment?</i>	<p>Before creating new systems based on electronic concept, there's a need to simplify the existing rules and eliminate what is not necessary. Simplification and Red Tape reduction in fact is the first step to lighten the burden for the civil society and to improve the efficiency of the system as a whole.</p> <p>New laws approval can be achieved by involving public and private partnership to enable a new balance between different and sometimes contrasting interests as the Italian PA is currently accomplishing within the "Digital Agenda for Europe" program proposed by the European Commission.</p>
<i>How was the private sector involved in the process (public outreach, commentary period, etc.)?</i>	<p>The Private sector, including logistics and forwarder companies, was invited to join public Institutions in the National Standing Committee on Trade Facilitation established in February 2010, after the organization of the first 2 national conferences on Trade Facilitation in Italy in 2008 and 2009, (the latter during the 14° UNCEFACT Forum in Rome -20-24 April 2009).</p> <p>All the participants to the Standing Committee have been divided into 4 different working groups to better analyze and understand all the existing procedures of the international trade, carrying out a SWAT analysis of the system. Each group was formed by institutional experts and sectorial experts.</p> <p>They have analyzed all the procedures and in particular the critical aspects, bottlenecks, identifying the problems, the consequences that might occur and proposing at the same time the best solution. Also according to the UNECE/UNCEFACT recommendations and standards, all these activities resulted in a collection of best practices and in a continuous activity of analysis and mapping and digitalization of all the procedures.</p>
<i>Were there any unexpected obstacles or complications that needed to be addressed?</i>	<p>Complications are quite normal when a radical simplification process has to be conducted, especially when different Admins are involved and the approval of a reform needs the involvement of many stakeholders. Legislation related to essential matters such as the tax system and the</p>

	public health require further consideration and harmonization.
	DETAILS OF SOLUTION (REMOVING MANUAL SIGNATURE LEGAL ENVIRONMENT)
<i>Please briefly note current laws and their role in removing manual signature / enabling electronic exchange of trade-related documents.</i>	<p>The Italian legal environment in this field was established progressively through since 1997: the DPR n.513 of 1997 - adopted in execution of article 15 of the law n. 59 of 15 March 1997 and later transposed in the DPR n. 445/2000 (Unified Body of Laws on the administrative documentation) - was the first normative act which established the validity of electronic signature for the subscription of documents.</p> <p>The 1999/93/CE Directive on the electronic signature was adopted by Italy through the legislative decree n.10 of 23 January 2002.</p> <p>Another important act adopted by the Italian legislation is the so-called “Digital Administration Code” (Codice dell’Amministrazione digitale -CAD), introduced by the legislative decree n. 82 of 7 March 2005, modified and amended in the following years. Despite its name, the Code applies to both private and public bodies.</p> <p>The Italian normative process in the field is still ongoing.</p>
	PRACTICAL EXPERIENCE IN USE OF THIS LEGAL ENVIRONMENT
<i>Resulting implementation in public sector (relating to trans-boundary trade)</i>	Even if the electronic transition is not yet operational, some of the critical points have been overcome especially in terms of communication between the private sector and the public Admin with the clarification of some rules that made companies life quite uneasy. More results are awaited as the implementation of the electronic system will go through different stages of development starting from the customs clearance operations, standard definition and implementation.
	CONTACT DETAILS
	<p>ITALIAN TRADE COMMISSION (ICE):</p> <ul style="list-style-type: none"> • PIER ALBERTO CUCINO PA.CUCINO@ICE.IT • GIOVANNA CHIAPPINI CARPENA G.CHIAPPINICARPENA@ICE.IT • SIMONLUCA DETTORI S.DETTORI@ICE.IT • ANNA BELMONTE A.BELMONTE@ICE.IT • CLAUDIA MANGHISI: C.MANGHISI@ICE.IT

ITALIAN ECONOMIC DEVELOPMENT MINISTRY:

- GRAZIANO SEVERINI:
G.SEVERINI@MISE.GOV.IT

806

807

Japan

Japan Association for Simplification of International Trade Procedures (Jastpro)

808
809
810
811

	BUSINESS / TRADE CONTEXT (VERY BRIEF)
<i>Please describe the business / trade context / need that was being addressed when you decided to move from physical to electronic signature. Why was this being put in place? What specific issues were being addressed?</i>	<p>Facilitation of business process by simplifying the process and in many cases , using ITC as to information exchange between B, C and G is effective.</p>
<i>What types of trade documents were involved – be specific/ authenticated?</i>	<p>Any information exchanged has to have the information of who provided the information. The ways of identifying of Who may vary depending on contents and purpose of usage of the information.</p> <p>1) In case of example B2G a user will log-in to NACCS(*) using a digital certificate issued by NACCS inc..</p> <p>(*) NACCS stands for ‘Nippon(Japan) Automated cargo and port consolidated system ’ which is a national single window for export and import related procedure(B2G and some part of B2B) done in domestic. (http://www.naccs.jp/e/index.html)</p> <p>2) In case of B2B a usual business procedure is to specify the name/company addressed at the top of e-mail contents and to put a name/company name / etc. at the bottom which may clarify from Who to Whom the e-mail was sent.</p> <p>Just as a guidance, the ministry of Internal Affairs and Communications issued an official report in which contains suggestion to use S/MINE at sending e-mail against spoofing problem. Using this is not a regulation and not yet commonly used in Japan.</p> <p>3) In case of B2B business, documents (irrespective of paper, fax or PDF) are sent ,usually , with a manual signature of individual with the information of his title and company name , typed or stamped especially in international trade.</p> <p>The certificate of the signature , if required by business</p>

	<p>partners , can be applied to and can be issued by many organizations of chambers of commerce and industry in Japan.</p> <p>Just as a guidance, a seal of an individual or of title with a name of an organization is used in domestic trade document in Japan.</p> <p>The certificate of the seal, if required, is applied to and issued by Legal Affairs Bureau.</p>
<i>Are there trade documents which do not legally require a signature?</i>	Above comment may be applied also to this question.
	LEGAL CONTEXT
<i>Type of legal system</i>	All laws, ordinances, regulations, rules have to be written. Jurisprudence will be for preparing how to apply to actual cases based on the written ones.
<i>What is the fastest that a legally enabling environment can be created?</i>	Skipped
<i>Environment for adding/amending laws</i>	<p>The constitution is the highest level of laws which can be altered by voting of the Diet then by voting of the nation according to the provisions of the constitution.</p> <p>Under the constitution, a law is proposed to the Diet by cabinet , members of the House of Representatives or members of the House of Councilors.</p> <p>Under the constitution and laws, cabinet, each prefecture, each city etc... can issue necessary ordinance/rules/regulations within each given responsibility range.</p>
	CONSULTATION / DEVELOPMENT (TRANSITION TO ELECTRONIC ENVIRONMENT)
<i>What considerations needed to be addressed before passing any laws creating the legally enabling environment?</i>	In general , it is important to involve all key players when a draft of a law, new or amendment, is made. The most responsible ministry/government agency usually prepares a table for discussion about operational and related legal issues. They invite key players who may include other

	<p>related ministries, government agencies, private sectors, experts with business/technical experience, scholars, etc. This table can be divided into necessary sub working groups depending on the discussed business area and its detailed level.</p> <p>For example, the ministry of Finance prepared a table whose one of discussion items was providing documents(including invoice) to customs in transmission of PDF to NACCS in addition of an existing function of transmitting the invoice data. After discussion with private sectors, this new function will start in October this year. Again the identification of the sender is confirmed by the user-id for NACCS as explained in the above answer.</p>
<p><i>How was the private sector involved in the process (public outreach, commentary period, etc.)?</i></p>	<p>Same as above comment</p>
<p><i>Were there any unexpected obstacles or complications that needed to be addressed?</i></p>	<p>Detailed and concrete explanation is skipped.</p>
	<p>DETAILS OF SOLUTION (REMOVING MANUAL SIGNATURE LEGAL ENVIRONMENT)</p>
<p><i>Please briefly note current laws and their role in removing manual signature / enabling electronic exchange of trade-related documents.</i></p>	<p>111) Digital signature (PKI) : ‘Act on Electronic Signature and Certification Business’ (Act No.102 of May 31 2000) into force on April 1,2001. This act includes ‘Definition of the term Electronic Signature and Authentication’ and that the Specified Certification business needs accreditation from competent minister. Competent ministers are the Minister of Internal Affairs and Communications, the Ministry of Justice and the Ministry of Economy, Trade and Industry.</p> <p>Under above law, Business process using PKI is increasing much in Japan where merit and cost effective in domestic business. It is not legally compulsory that PKI should be used in B2B.</p> <p>This PKI is supported by Japan government and its scope is to cover domestic business.</p> <p>PKI process between C2G is called ‘GPKI :Government Public key Infrastructure’ whose operation started in April 2001.</p>

	<p>222) A law related with allowing keeping document in electronic media (So called e-document law) became effective April 1, 2005. (Act of No.149 and No.150 in 2004) The documents(*) which legally had to be archived/stored by paper documents can be in electronic media which includes both cases of the data of originally created electronically and of the image data by scanning the paper document.</p> <p>(*) There are some exceptions about kinds of documents.</p> <p>333) NACCS (Nippon Automated Cargo and Port Consolidated System) as National Single Window in Japan:</p> <p>Electronic business process using NACCS has been increasing instead of manual processing.</p> <p>The Special Law of Customs Procedures for Air Cargo was changed to the "Act on Processing, etc. of Business Related to Import and Export by Means of Electronic Data Processing System (NACCS Special Law)" in 1991.</p> <p>Sea Cargo related process using Sea-NACCS started in 1991.</p> <p>The Special Law of Customs Procedures through the Electronic Data Processing System was changed to the "Act on Special Provisions for Customs Procedure by Means of Electronic Data Processing System" (privatization of the incorporated administrative agency NACCS inc.) in 2008.</p> <p>This reform was done with a view of promoting an efficient import/export related operation under the new generation of Single Window in Japan. Not only Government (not only customs but also other government agencies), carriers, forwarders, traders are exchanging information via NACCS.</p> <p>(http://www.naccs.jp/e/aboutcenter/history.html)</p>
	<p>PRACTICAL EXPERIENCE IN USE OF THIS LEGAL ENVIRONMENT</p>
<p><i>Resulting implementation in public sector (relating to trans-boundary trade)</i></p>	<p>Please refer to the comments in above question.</p>
	<p>Remark: All above explanation is non-exhaustive and</p>

	subject to update/correction by experts from relevant sectors.
	<p>CONTACT DETAILS</p> <p>Reported by Mitsuru Ishigaki JASTPRO (m-ishigaki@jastpro.or.jp)</p>

812

Republic of Korea

	BUSINESS / TRADE CONTEXT (VERY BRIEF)
<i>Please describe the business / trade context / need that was being addressed when you decided to move from physical to electronic signature. Why was this being put in place? What specific issues were being addressed?</i>	<p>Legally enabling environment of electronic documents provides great innovative values in business and trade. The paperless policy was facilitated in both legal and technical context.</p> <p>For the papeless transition in society, the authentication of e-documents, from its creation to its disposal, is one of critical issues.</p>
<i>What types of trade documents were involved – be specific/ authenticated?</i>	Three types of trade documents (Letter of Credit, e-Negotiation Application, e-Bill of lading) have the legal obligation of authentication (under the Electronic Trade Facilitation Act).
<i>Are there trade documents which do not legally require a signature?</i>	Most of e-trade documents are generally signed for the purpose of the protection from probable dispute, although it's not legal obligation (under the Electronic Trade Facilitation Act).
	LEGAL CONTEXT
<i>Type of legal system</i>	Civil Law, General Law, Commercial Law
<i>What is the fastest that a legally enabling environment can be created?</i>	Legal recognition in General Law such as 'Digital Signature Act' and 'Framework Act on Electronic Document and Electronic Commerce'
<i>Environment for adding/amending laws</i>	'Framework Act on Electronic Document and Electronic Commerce' was added its legal systems regarding authentication. Some of Civil and Commercial laws were ammended to stipulate the legal effect of e- documents in each domain area.
	CONSULTATION / DEVELOPMENT (TRANSITION TO ELECTRONIC ENVIRONMENT)
<i>What considerations needed to be addressed before passing any laws</i>	<ul style="list-style-type: none"> • Analysis of the obstacles (practices, customs or jurisdiction etc.) for paperless transition <ul style="list-style-type: none"> ○ Review legal scheme and electronic environment.

<p><i>creating the legally enabling environment?</i></p>	<ul style="list-style-type: none"> • Consultation about the authentication of e-document <ul style="list-style-type: none"> ○ Define the trustworthy environment using e-document as legal source; and ○ Research a trusted solution to minimize the least risks, errors and uncertainties given in the electronic environment; and ○ Plan strategies as a cooperative model between private and public sector. (Especially, the third party is easy to prove it neutrally and the public sector can organize the overall scheme of trusted system). • Development of a trusted system <ul style="list-style-type: none"> ○ Develop regulations and restrictions; and ○ Develop a technical guidance needed to ensure a trusted system. • Facilitation of TTP (Trusted Third Party) service <ul style="list-style-type: none"> ○ Facilitate that TTP or private sector provide the service in compliance with regulations and technical guidance; and ○ Facilitate that public sector assesses regularly the quality of trusted system and provides the audit.
<p><i>How was the private sector involved in the process (public outreach, commentary period, etc.)?</i></p>	<p>The private sector applies for TTP services in compliance with technical guidelines.</p> <p>Public sector evaluates its compliance and designates it as a TTP.</p>
<p><i>Were there any unexpected obstacles or complications that needed to be addressed?</i></p>	<p>There is no mutual recognition of authentication beyond national PKI among cross-boarder's e-transactions.</p>
	<p>DETAILS OF SOLUTION (REMOVING MANUAL SIGNATURE LEGAL ENVIRONMENT)</p>
<p><i>Please briefly note current laws and their role in removing manual signature / enabling electronic exchange of trade-related documents.</i></p>	<ul style="list-style-type: none"> • Digital Signature Act (1999), (2001),(2005),(2008),(2010), (2011) <ul style="list-style-type: none"> ○ Purpose of legislation is to improve security and reliability of e- document. It provides the authentication, identification and integrity to facilitate e- commerce, e- government and good life of citizen. ○ This act refers to MLES (Model Law of e-Signature) of UNCITRAL. ○ This act requires legal effect by utilizing digital signature, certified authority system of digital signature and etc. ○ KISA (Korea Information Security Agency) organizes certified authority system. ○ This act establishes a process for interested group to :

- keep control of the protection from kinds of risks such as cyber infringement, unaccepted access and disaster; and
 - issue a certificate to identify a particular person by hash algorithm ; and
 - record the activities of user's certificate and its certified system.

- **Framework Act on Electronic Document and Electronic Commerce** (1999),(2002),(2005),(2006), (2007), (2008), (2009), (2012)
 - Purpose of this act is to stipulate legal relations of the e-commerce, ensuring its security and reliability, and laying the foundation for its promotion.
 - This act refers to MLEC (Model Law of e-Commerce) of UNCITRAL
 - This act requires the legal effect by utilizing e-document, trusted third party repository, trusted electronic address and certification of communication, etc.
 - NIPA (National IT Industry Promotion Agency) organizes overall scheme of trusted system regarding electronic documents and electronic commerce.
 - This act establishes the process and rules for interested group to :
 - keep control of the protection from the kinds of risks such as cyber infringement, unaccepted access and disaster ; and
 - issue certificate of authenticity of e-document ; and
 - issue certificate of communication of e-document.

- **Electronic Government Act** (2010), (2011), (2012)
 - Its purpose is for required federal agencies to provide e-government services and manage administrative documents electronically.
 - This act refers to Digital Signature Act.
 - This act requires the electronic administrative document and ESI (Electronically Stored Information) format.
 - This act establishes procedures and rules for federal agencies to:
 - request a civil appeal in electronic format ; and
 - confirm the civil affair document and required documents in electronic format ; and
 - confirm the identification of a client of civil affair under Digital Signature Act ; and
 - keep control of administrative document in electronic format ; and
 - stipulate the legal effect of using the electronic documents.

- **Electronic Financial Transaction Act** (2006), (2007), (2008), (2010), (2011), (2012)
 - The purpose of this act is to contribute to ensuring the security and reliability of e- financial transactions by clarifying their legal relations and to promoting financial conveniences for people and developing the national economy by creating a foundation of the sound development of electronic financial industry.
 - This act refers to Digital Signature Act.
 - This act requires the right and responsibility of person concerned about electronic financial transaction, electronic money and the legal effect of electronic payment etc.
 - This act establishes some regulations, guidelines and procedures for financial agencies and financier to:
 - access the system media and confirm the identification and permission of a client and the intent of transaction.
 - handle the least errors and/or accidents during e- financial transactions

- **Act on the Use, etc. of Electronic Document in Civil Litigation** (2010)
 - Its purpose is to promote informatization of civil litigation, etc. and enhances swiftness and transparency thereof, thereby contributing to realizing people's rights, by prescribing fundamental principles and procedures concerning the use of electronic documents in civil litigation, etc.
 - This act refers to Digital Signature Act and Electronic Government Act
 - This act requires digital signature used in judicial case
 - This act establishes procedures for 'Office of Court Administration' to:
 - execute civil litigation by electronic document; and
 - register and submit electronic documents to a court; and
 - record the cases of civil litigation in electronic format.

- **Electronic Trade Facilitation Act** (2005),(2007), (2008), (2009), (2011)
 - The purpose is to simplify trade procedures, rapidly circulate trade information and costs of handing trade business by creating grounds for electronic trade and facilitating the wide use.
 - This act refers to the Digital Signature Act and the

	<p>Framework Act on Electronic Document and Electronic Commerce</p> <ul style="list-style-type: none"> ○ KITA (Korea International Trade Association) organizes electronic trade portal called as ‘uTraceHub’. ○ This act requires electronic trade document, electronic trade service provider and electronic trade portal ○ This act establishes rule that electronic trade portal provides following services: <ul style="list-style-type: none"> ▪ notice about the Letter of Credit, ▪ e-Negotiation Application, ▪ issuance of e-Bill of Lading ○ This act establishes process for trader to manage electronic trade document such as: <ul style="list-style-type: none"> ▪ archive el-trade documents ; and ▪ certificate of authenticity. <ul style="list-style-type: none"> ● Value-Added Tax Act Act No. 9268(2008) <ul style="list-style-type: none"> ○ NTS (National Tax Service) organizes the value-added tax system ○ This act refers to ‘Digital Signature Act’ and ‘Framework Act on Electronic Document and Electronic Commerce’ ○ This act requires e-tax bills document ○ This act establishes a process for business enterprise to <ul style="list-style-type: none"> ▪ keep control of e-tax bills in electronic format ; and ▪ declare e-tax bills to NTS via Internet. ● Regulation Implementation of the Provisions of the Commercial Act Regarding Electronic Bills of Lading , Presidential Decree No.22467(2010) <ul style="list-style-type: none"> ○ The purpose is to provide for matter delegated pursuant to Article 862 of the Commercial Act ○ This act refers to Digital Signature Act ○ This act requires register agencies, electronic registry of electronic bills of lading ○ This act establishes the process for trading companies to : <ul style="list-style-type: none"> ▪ issue electronic bills of lading ; and ▪ transfer electronic bills of lading.
	<p>PRACTICAL EXPERIENCE IN USE OF THIS LEGAL ENVIRONMENT</p>
<p><i>Resulting implementation in public sector (relating to trans-boundary trade)</i></p>	<p>The ‘<i>digitally signed document</i>’ during electronic transactions can be considered as the legal source of electronic document under the Digital Signature Act and the Framework Act on Electronic Document and Electronic Commerce. However there are some difficulties in real world, because digital signature is only valid within certain period.</p>

For the purpose of ‘paperless transition’ in society, in Korea there are two practical solutions such as ‘TTPR’ and ‘Trusted address and sharp (mail) service’ in order to reduce the probable disputes with cause for electronic format or transactions. These are the trusted service in a model of PPP (Private Public Partnership) guaranteed by the national laws.

- **TTPR (Trusted Third Party Repository)**

There is a big hurdle for paperless transition. Even if the electronic document is properly produced during e-business, people tends preserve it as paper format keeping the legal evidence. Because it is difficult to identify its original or changeable source, a solution is needed. TTPR provides an easy way to guarantee the ‘*authenticity of e-documents*’ in compliance with legal requirements by expertise of archive (and disposal) for the long term.

In 2006 the ‘Framework Act on Electronic Document and Electronic Commerce’ was revised to state legal grounds (Article 5-1, 31) that a TTPR can issue the certificate of authenticity about e-document archived in TTPR. In addition, this law includes its regulations, technical guidelines and audit scheme needed to guarantee a trusted system.

In Korea there are 6~7 TTPRs for archiving. TTPRs are creating new value added services of substituting for previously paper based work such as clients’ subscription procedure at insurance companies, credit card companies, stock brokers and banks, the clients’ admission/leaving procedure at hospitals and clinics, lots of issuance procedures at universities, educational institutes or test laboratories and so on. And also it could be expected new service model in cloud environments.

- **Trusted address and sharp (mail) service**

‘The signed documen’t during e-transactions can be considered as a legal source. However after finalizing the valid period of electronic signature or getting rid of electronic signature, it is difficult to prove its business context –e-documents resulted from reliable communications with identified partners. Therefore, in advance it is needed to realize a provable solution to verify its authentication – *‘the e-document born through reliable communications’*.

In 2012 the ‘Framework Act on Electronic Document and Electronic Commerce’ was revised to state legal grounds about the trusted address (Article 18- 4) and trusted communication system. Trusted address, compared with e-mail address, guarantees the reliable communications for legal effect. TTP (Trusted Third Party)s provide the trusted communications called ‘sharp mail service’ by using trusted address. Although it could be compared with ‘registered mail’, tey are really different in a way of message handling.

In Korea there are now 4~5 TTPs for trusted communication service. It can provide trusted services applied to

	<p>kinds of business models in G2P, B2B, P2P, B2P and so on. However, not yet this service is incorporated with TTPR. The further combination of these services could provide a way to prove the authentication of e-document from its creation to archive (and disposal).</p> <ul style="list-style-type: none"> E-Customs and e-Trade Services In Korea, there are two portal services; ‘UNI-PASS’ and ‘uTradeHub’. The paperless trade service portal called ‘uTradeHub’ has been operated by KITA (Korea International Trade Association) since 2003. And electronic clearance portal system called ‘UNI-PASS’ (previously, Internet Clearance 2005 and EDI Auto Clearance 1992) has been serviced by KCS (Korea Customs Service) since 2010. These portal services process electronically overall customs and trade affairs such as clearance, cargo management, and duty collection, marketing, checking conditions, foreign exchange, customs clearance, logistics and payment. For handling above activities, these systems are interlinked with networks of trading parties concerned, domestic banks, foreign bank, the Korea Financial Telecommunications and Clearings Institute, the Korea Customs Services and logistics companies. For the international trade, there are some difficulties of digitally signed documents depending on NPKI (National Public Key Infrastructure). For the handling it, it is needed that digital signature should be recognized mutually with other countries and its legal effect should be equal globally in forth coming days.
	<p>CONTACT DETAILS</p>
	<p>NIPA(National IT Industry Promotion Agency)</p> <ul style="list-style-type: none"> JASMINE JANG jasmine@nipa.kr

Turkey

TR

816

817

818

Ministry of Customs and Trade

	BUSINESS / TRADE CONTEXT (VERY BRIEF)
<i>Please describe the business / trade context / need that was being addressed when you decided to move from physical to electronic signature. Why was this being put in place? What specific issues were being addressed?</i>	The establishment of an e-signature system provides electronic signing of customs declarations, that results in a safer and faster international trade.
<i>What types of trade documents were involved – be specific/ authenticated?</i>	Customs declarations (Single Administrative document) Transit Accompanying Document (NCTS)
<i>Are there trade documents which do not legally require a signature?</i>	They all require a customs administrations' signature procedure.
	LEGAL CONTEXT
<i>Type of legal system</i>	The electronic signature Law of 2004
<i>What is the fastest that a legally enabling environment can be created?</i>	By using electronic systems
<i>Environment for adding/amending laws</i>	
	CONSULTATION / DEVELOPMENT (TRANSITION TO ELECTRONIC ENVIRONMENT)
<i>What considerations needed to be addressed before passing any laws creating the legally enabling environment?</i>	
<i>How was the private sector involved in the process (public outreach, commentary period, etc.)?</i>	Private sector is able to use electronic signatures as well.

819

<i>Were there any unexpected obstacles or complications that needed to be addressed?</i>	No.
	DETAILS OF SOLUTION (REMOVING MANUAL SIGNATURE LEGAL ENVIRONMENT)
<i>Please briefly note current laws and their role in removing manual signature / enabling electronic exchange of trade-related documents.</i>	The above mentioned Law provides to use both of them.
	PRACTICAL EXPERIENCE IN USE OF THIS LEGAL ENVIRONMENT
<i>Resulting implementation in public sector (relating to trans-boundary trade)</i>	It's crucial for simplification of trade.
	CONTACT DETAILS
	Ministry of Customs & Trade DG for Risk Management & Control Department of e-customs

821
822
823

United States of America

United States Customs and Border Protection (CBP)



	BUSINESS / TRADE CONTEXT (VERY BRIEF)
<i>Please describe the business / trade context / need that was being addressed when you decided to move from physical to electronic signature. Why was this being put in place? What specific issues were being addressed?</i>	The greatest need addressed in the decision to move from a physical signature to electronic signature was the legislative mandate (see reference to the Mod Act below) to manage business improvements in customer service, trade facilitation, and compliance with regulations and tariffs. The ultimate goal for CBP was improved border enforcement and trade compliance under U.S. laws and regulations, while simultaneously creating greater efficiencies and facilitation of legitimate trade and travel.
<i>What types of trade documents were involved – be specific/ authenticated?</i>	The importation of goods into the United States, is generally a two-part process consisting of 1) filing the cargo release documents necessary to determine whether merchandise may be released from CBP custody, and 2) filing the entry summary documents that pertain to merchandise classification, duty, taxes, and fees. For the most part, the documents involved were for purposes of entry summary. Currently, over 99 percent of all entry summaries are filed electronically. The only documents CBP still collects which would require wet ink signatures are those forms which CBP collects on behalf of other agencies, entry papers (i.e., consumption entry and the invoice), and any classified documents.
<i>Are there trade documents which do not legally require a signature?</i>	See response above. Everything (with the exception of entry papers and classified documents) that is filed electronically with CBP gets an electronic signature.
	LEGAL CONTEXT
<i>Type of legal system</i>	Common Law
<i>What is the fastest that a legally enabling environment can be created?</i>	The fastest path to a legally enabling environment is via legislation and/or Presidential Executive Order. The legislation will usually provide a period of time by which the requested change must take place. It is the responsibility of federal agencies to make the necessary revisions/updates to their regulations to implement the legislation.
<i>Environment for adding/amending laws</i>	Security/health based legislation is “fast tracked” as necessary. Other legislation that does not address security/health based concerns follows a more traditional path. Once a bill is introduced, it is sent into the appropriate subject matter Committee (separately, in both the House and Senate) for review. The respective Committee can choose to

	<p>table the bill or make recommendations and put it to a vote. This is the time when the bill will be shared with other organizations for feedback/input.</p> <p>Separately, the Senate and the House will debate the bill, offer amendments and cast votes. If the bill is defeated in either the Senate or the House, the bill dies. It is not unusual for the House and the Senate to pass the same bill, but with different amendments. In these cases, the bill goes to a conference committee to work out differences between the two versions of the bill. Then the bill goes before all of Congress for a vote. If a majority of both the Senate and the House votes for the bill, it goes to the President for approval. If the President approves the bill and signs it, the bill becomes a law. However, if the President disapproves, he can veto the bill by refusing to sign it. Congress can try to overrule a veto. If both the Senate and the House pass the bill by a two-thirds majority, the President's veto is overruled and the bill becomes a law. Once the law is enacted the Administration will usually provide a broad framework of guidance to ensure implementation of the legislation.</p>
	<p>CONSULTATION / DEVELOPMENT (TRANSITION TO ELECTRONIC ENVIRONMENT)</p>
<p><i>What considerations needed to be addressed before passing any laws creating the legally enabling environment?</i></p>	<p>Prior to advocating a legally enabling environment that will promote or require a transition to an electronic environment; the agency must conduct a thorough review of the paper based processes to determine whether any are suitable for conversion to electronic signature. If a determination is made that some processes would be suited for conversion, the agency must assess whether there are any existing gaps in the paper based process that can be mitigated by conversion to electronic. An additional consideration is the level of protection that will be required for the government and the potential of risk or liability for the agency. Also important is a review of the current legal schema to determine whether there are any existing legislative and/or regulatory restrictions. Per guidance from the Office of Management and Budget (OMB), agency considerations of cost, risk and benefit, as well as any measures taken to minimize risks, should be commensurate with the level of sensitivity of the transaction (i.e., low risk information processes may need only minimal safeguards while high risk processes may need more). Impact to stakeholders must also be assessed and consultations with all impacted parties must be coordinated.</p>
<p><i>How was the private sector involved in the process (public</i></p>	<p>Yes, the private sector must certainly be part of the process. Government should, in consultation with other agencies and</p>

<p><i>outreach, commentary period, etc.)?</i></p>	<p>private sector, develop practical guidance on the legal considerations related to agency use of electronic signatures so that appropriate assessments can be made in terms of goals and acceptance of those goals by all vested parties. In CBP, any change from a paper based process to an electronic process is precipitated by a legal notice announcing to the trade community the changes CBP would like to implement. The trade community is given an opportunity to provide written comments. In the interim CBP reaches out to all the impacted industry sectors and coordinates outreach/engagement prior to any decision making.</p>
<p><i>Were there any unexpected obstacles or complications that needed to be addressed?</i></p>	<p>Obstacles include differing legislative mandates across federal agencies; divergent trade needs; lack of adequate resources (both financial and human) to support the necessary changes, and technical upgrades that must be made on both sides (government and trade) to support the needed changes.</p>
	<p>DETAILS OF SOLUTION (REMOVING MANUAL SIGNATURE LEGAL ENVIRONMENT)</p>
<p><i>Please briefly note current laws and their role in removing manual signature / enabling electronic exchange of trade-related documents.</i></p>	<ul style="list-style-type: none"> • Computer Security Act of 1987, Pub. L. No. 100-235, 40 U.S.C. 1441: Legislation passed to improve the security and privacy of sensitive information in Federal computer systems and to establish a minimum acceptable security practices for such systems. Requires the creation of computer security plans, and the appropriate training of system users or owners where the systems house sensitive information. • Paperwork Reduction Act of 1995: Required each Federal agency to establish a process, independent of program responsibility, to evaluate proposed collections of information; manage information resources to reduce information collection burdens on the public; and ensure that the public has timely and equitable access to information products and services. • Government Paperwork Elimination Act (GPEA), Pub. L. No. 105, 1998, codified as 44 U.S.C. 350: Required federal agencies to provide for the option of the electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper; and the use and acceptance of electronic signatures when practicable). • Electronic Records and Signatures in Global and National Commerce Act (E-SIGN), Pub. L. 106-229, 2000, 15 U.S.C. 7001(E-SIGN): Eliminates legal barriers to the use of electronic technology to form

and sign contracts, collect and store documents, and send and receive notices and disclosures. E-SIGN applies broadly to Federal and state statutes and regulations governing private sector activities. Laws and regulations that are primarily governmental and do not relate to business, commercial or consumer transactions are not within the scope of this legislation; they are instead addressed by the Government Paperwork Elimination Act.

- U.S. Customs and Border Protection Specific Empowering Legislation:
 - Customs Modernization Act (the “Mod Act”), Pub. L. 103-182, December 8, 1993, amending title 19 U.S.C. 1508, 1509 and 1510, formally Title VI of the North American Free Trade Agreement Implementation: One of the most sweeping regulatory reform legislations, amending the Tariff Act of 1930 and related laws. Introduced two new Customs concepts known as "informed compliance" and "shared responsibility." These concepts are premised on the idea that in order to maximize voluntary compliance with Customs laws and regulations, the trade community needs to be clearly and completely informed of its legal obligations. An overarching goal of the Mod Act was to place a greater responsibility upon the trade community to exercise “reasonable care” in complying with import requirements.
 - The principal section of the Mod Act addressing automation was codified under 19 U.S.C. 1411-1414 (promulgated by CBP under the National Customs Automation Program (NCAP) testing provision, 19 CFR 101.9). NCAP provides U.S. Customs and Border Protection with an automated electronic system to process commercial importations and facilitate business improvements with the trade community.
 - Among other statutes, the Mod Act amended Section 484 of the Tariff Act of 1930. Added provision (d) (1) providing that: Entries shall be signed by the importer of record, or his agent, unless filed pursuant to an electronic data interchange system. If electronically filed, each transmission of data shall be certified by an importer of record or his agent, one of whom shall be resident in the United States for purposes of receiving service of process, as being true and correct to the best of his knowledge and belief, and such transmission shall be binding in the

	<p>same manner and to the same extent as a signed document. The entry shall set forth such facts in regard to the importation as the Secretary may require and shall be accompanied by such invoices, bills of lading, certificates, and documents, or their electronically submitted equivalents, as are required by regulation.</p> <ul style="list-style-type: none"> ➤ The Mod Act also allowed for the submission of information through a CBP authorized electronic data interchange system in all statutes that previously required documents or forms so that the electronic transmission of data could replace submission of the documents. Moreover, the Mod Act did not specify any one system purposefully so we can use any system we approve. ➤ Under the authority of the Mod Act, we also allow approved parties to convert and store original paper documents into an electronic medium and store them electronically if CBP approves an alternative storage method. ➤ The Mod Act was subsequently amended by the Trade Act of 2002 to include, among other things, the following change (2002—Subsec. (b). Pub. L. 107–210): Struck out a former second sentence which read as follows: “Participation in the Program is voluntary.” Inserted a new second sentence which now reads: The Secretary may, by regulation, require the electronic submission of information described in subsection (a)... • Security and Accountability for Every Port Act of 2006 (P.L. 109-347 (Section 405), October 13, 2006, (SAFE Port Act): Required the Secretary of the Treasury to oversee an interagency initiative to establish a “single portal system,” to be known as the” International Trade Data System” (ITDS) and to be operated by the United States Customs and Border Protection. This unified data system is to electronically collect and distribute import and export data required by government agencies that license or clear the import or export of goods.
	<p>PRACTICAL EXPERIENCE IN USE OF THIS LEGAL ENVIRONMENT</p>
<p><i>Resulting implementation in public sector (relating to trans-boundary trade)</i></p>	<p>There are a number of ways in which CBP is currently successfully using electronic signatures.</p> <ul style="list-style-type: none"> • The ACE Secure Data Portal is a web-based capability providing a single, centralized on-line

	<p>access point to connect CBP, the trade community and government agencies. Once a Portal Account is established, trade members can electronically submit specified data and/or documentation/forms needed during the cargo importation process. ACE authenticates the electronic documents that it receives by comparing certain fields in the message to a user profile established at the time of registration. The profile includes, among other things, both the filer code and password chosen by the filer. This “trusted” profile is used during authentication (Port, Filer Code, password).</p> <ul style="list-style-type: none"> • The Document Image System (DIS) provides the trade community the ability to electronically submit imaged copies of specified documents and forms so they can be processed and stored electronically eliminating the need to process and store paper documents and forms. • EDI data-transmissions (through ABI – Automated Broker Interface, for example)- Another method by which trade members can submit data to CBP. To use ABI, a brokerage or importer must request or already possess a “filer code.” Once a filer code has been issued, the brokerage/importer must submit a Letter of Intent indicating intent to transmit data via EDI. Any party transmitting data with CBP must also sign an Interconnection Security Agreement (ISA). Data is transmitted using a Virtual Private Network (VPN), a means of communication from one computer to another over a public telecommunications network that relies on encryption to secure the content of transmissions.
	<p>CONTACT DETAILS</p>
	<p>Josephine Baiamonte Branch Chief, Change Management and Legal Policy, ACE Business Office U.S. Customs and Border Protection Email: josephine.baiamonte@dhs.gov</p>

825
826
827
828

Recommendation 14 “Authentication of Trade Documents by Means Other Than a Manual-Ink Signature” Template for comments and observations

Please return completed templates to Working Group Chair, Lance THOMPSON: lance.thompson@conex.net

Date submission:	
------------------	--

829
830

Please make all comments using this template.
Please propose suggested changes in order to make the Recommendation Draft align with your comments.

Ref. (leave blank)	Draft version number	Line numbers	Type of comment ¹	Comments	Proposed changes	Working Group Observations (leave blank)

831
832
833

¹ Types of comments: ge = general; te = technical; le = legal; ed = editorial
(This document is inspired by the ISO/IEC/CEN/CENELEC electronic balloting commenting template/version 2012-03)