

1 **Recommendation for ensuring legally significant trusted**  
2 **trans-boundary electronic interaction**  
3  
4  
5 draft  
6 version 0.3

7	Contents	
8		
9	Foreword.....	3
10	Executive summary .....	3
11	1. Recommendation № ____ : Recommendation for ensuring legally significant trusted	
12	trans-boundary electronic interaction .....	3
13	1.1. Scope.....	3
14	1.2. Benefits.....	3
15	1.3. Use of International Standards .....	3
16	1.4. Recommendation .....	3
17	2. Guidelines on how to implement the recommendation .....	4
18	2.1. Terms and Definitions.....	4
19	2.2. Common Trust Infrastructure establishment principles.....	5
20	2.3. Common Trust Infrastructures coordination approaches.....	6
21	2.4. Trust infrastructures services technical interoperability ensuring approaches.....	8
22	2.5. Trust infrastructures services levels of trust.....	8
23	2.6. Communication with organizations in different areas of standardization .....	8
24	3. ANNEX 1.....	9
25	Terms and Definitions .....	9
26		

27 **Foreword**

28

29 **Executive summary**

30

31

32 **1. Recommendation № \_\_\_\_ : Recommendation for ensuring**  
33 **legally significant trusted trans-boundary electronic**  
34 **interaction**

35

36 **1.1. Scope**

37 This Recommendation seeks to encourage the use of electronic data transfer in international  
38 trade scenarios by recommending Governments the principles of establishing and operating  
39 regional and international coordination organizations for ensuring trust in international  
40 exchange of data and electronic documents between authorized bodies.

41

42 **1.2. Benefits**

43 Harmonized regional and international coordination based on common principles will provide  
44 a smooth, transparent and liable environment for electronic activities in trans-boundary trade  
45 scenarios. This will make it possible to attach legal significance to an electronic interaction  
46 for legal bodies and economic operators regardless of their location and jurisdiction.

47

48 **1.3. Use of International Standards**

49 The use of international standards can play a key role in larger acceptance of chosen solutions  
50 and eventually interoperability. Insofar as possible, legal and private actors who intend to use  
51 electronic data transfer in international trade scenarios should try to make use of existing  
52 international standards. Technical standards which were able to be identified during the  
53 development of this Recommendation are referenced in Annex B.

54

55 **1.4. Recommendation**

56 The existing natural peculiarities (historical, cultural, political, economic, technical, etc) of  
57 different world regions cause also different level of trust within these regions concerning  
58 *electronic interaction*.

59 To Governments and entities engaged in the international trade and movement of goods,  
60 providing services and payment processing and willing a tighter, more transparent, effective  
61 and easier co-operation concerning *electronic interactions*, the United Nations Centre for  
62 Trade Facilitation and Electronic Business (UN/CEFACT) recommends establishing and  
63 using a dedicated Common Trust Infrastructure (hereinafter CTI).

64 The primary objective of CTI is ensuring *legally significant electronic interactions* between  
65 its users by providing *trust services* of different qualifications (basic, medium, high) to the  
66 participants of *electronic interaction*.

67 The CTI is a fundamental, easily scalable platform providing a unified access to trust services.  
68 Herewith, the existing electronic systems are taken into account, so the requirements to their  
69 updating for connecting to the CTI are expected to be minimal.

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

- 71 – CTI establishment principles;  
72 – CTI coordination approaches;

- 73 – approaches ensuring technical interoperability of CTI services;  
74 – levels of trust provided by CTI;  
75 – standardization organizations to co-operate with.  
76

## 77 **2. Guidelines on how to implement the recommendation**

78  
79

### 80 **2.1. Terms and Definitions<sup>1</sup>**

81 For the purposes of this document the following terms apply:

#### 82 ***Common Trust Infrastructure (CTI)***

83 infrastructure ensuring the *legal significance* of transboundary *electronic interaction*. CTI  
84 provides a set of *trust services* harmonised on the legal, organisational and technical /  
85 technological levels to its users.

86

#### 87 ***electronic interaction***

88 – a way of *information interaction* based on use of information and communication  
89 technologies (ICT). ICT refers to technologies that provide information processing  
90 (creation, access, transformation, transmission, destruction, etc.) in the telecommunication  
91 context<sup>2</sup>.

#### 92 ***legal significance (of an action)***

93 – a property of an action (of a process) to originate (to result in) documents (*data unit*)  
94 possessing *legal validity*.

95

#### 96 ***legal validity (of a document, or, generally, of data)***

97 – a property of a document (*data unit*) to be applicable for judicature, i.e. be deemed to have  
98 satisfied the requirements of applicable law. The *legal validity* is conferred to a document  
99 by the legislation in force, by the authority of its issuer and by the established order of its  
100 issuing (e.g. it shall be usable for a subsequent reference).

#### 101 ***level of qualification (of a service)***

102 – a property of a *service* to evidently fulfil a pre-defined set of requirements on it.

103 A service may be a *trust service* or an *authentication service* or any other kind of services,  
104 to which this term may be applicable.

---

<sup>1</sup> *Italic face* tags the terms defined in the current Recommendation

<sup>2</sup> ICT is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication mediums

105 There may be different, usually incremental *qualification levels* of a service like ‘zero’,  
106 ‘basic’, ‘medium/advanced’, ‘high/qualified’ etc. The lower is the *level of trust* between  
107 the participants of *information interaction*, the higher might be demand on the  
108 *qualification level* of *services* used by them.

109 ***levels of trust*** (between the participants of *information interaction*)

110 – a societal function determining the degree of trust between the participants of *information*  
111 *interaction*. Depending on an established or felt level of trust, the participants of  
112 *information interaction* are prepared to share a certain amount of resources and to jointly  
113 use certain infrastructures.

114 For example, with conditionally ‘high’ or ‘medium’ level of mutual trust between the  
115 participants, they may be prepared to jointly use centralized international services applied  
116 according to the standards agreed upon. In case of conditionally ‘low’ level of trust, the  
117 participants may be prepared to use only services built according to the decentralized  
118 principle – own services of each participant with a kind of link between them.

119 ***trust service***

120 – (high level definition) - an electronic service purposing to ensure a certain *level of trust*  
121 between the participants of *electronic interaction*.

122 or

123 – (lower level definition, will be clarified during Recommendation development) -

124 1. a service that is reasonably secure from intrusion and misuse; provide a reasonable  
125 level of availability, reliability, and correct operation; are reasonably suited to performing  
126 their intended functions; and enforce the applicable security policy.

127 2. trust service is a set of requirements and enforcement mechanisms for parties to  
128 authenticate and exchange information

129 3. eIDAS definition.

130 ***trusted electronic interaction***

131 – the exchange of any data in electronic form in such a way that a user of these data  
132 undoubtedly accepts them according to its Operational Policy. It is a matter of a concrete  
133 Operational Policy, which way is considered as a *trusted* one. Hence, the determination of  
134 the trustworthy of some data varies from one concrete case to another. Trusted electronic  
135 interaction is provided by using *trust services*.

136

137 **2.2. Common Trust Infrastructure establishment principles**

138

139 – **Scalability.** The CTI is established in such a way that it can be easily scaled. It broadens  
140 easily at any level of consideration due to the accession of new participants, such as new

- 141 jurisdictions, new supranational participants, new operators of trust services, and register  
142 systems.
- 143 – **Traceability.** Any fact of electronic data exchange within the CTI should be fixed and  
144 available for conflict resolutions if necessary.
  - 145 – **Cost efficiency.** While the CTI architecture variants comparison the risk analysis should  
146 be taken into account.
  - 147 – **Complexity.** Coherent elaboration of legal, organizational and technological issues should  
148 be done within CTI establishment. A complex description allows correct functioning of  
149 the system as a whole and its single elements.
  - 150 – ...##

151–  
152

### 153 **2.3. Common Trust Infrastructures coordination approaches**

154 *Identify the principles of establishing and operating regional and international coordination*  
155 *organizations for ensuring trust in infrastructures that satisfy organizational and*  
156 *administrative regulation of legally significant trans boundary electronic data exchange*

157 *Identify the underlying principles and content for Model MoUs/Agreements between two or*  
158 *more countries regarding Mutual Recognition of Digital and Electronic Signature*  
159 *Certificates*

160

161 There are three levels of coordination: legal, organizational and technological.

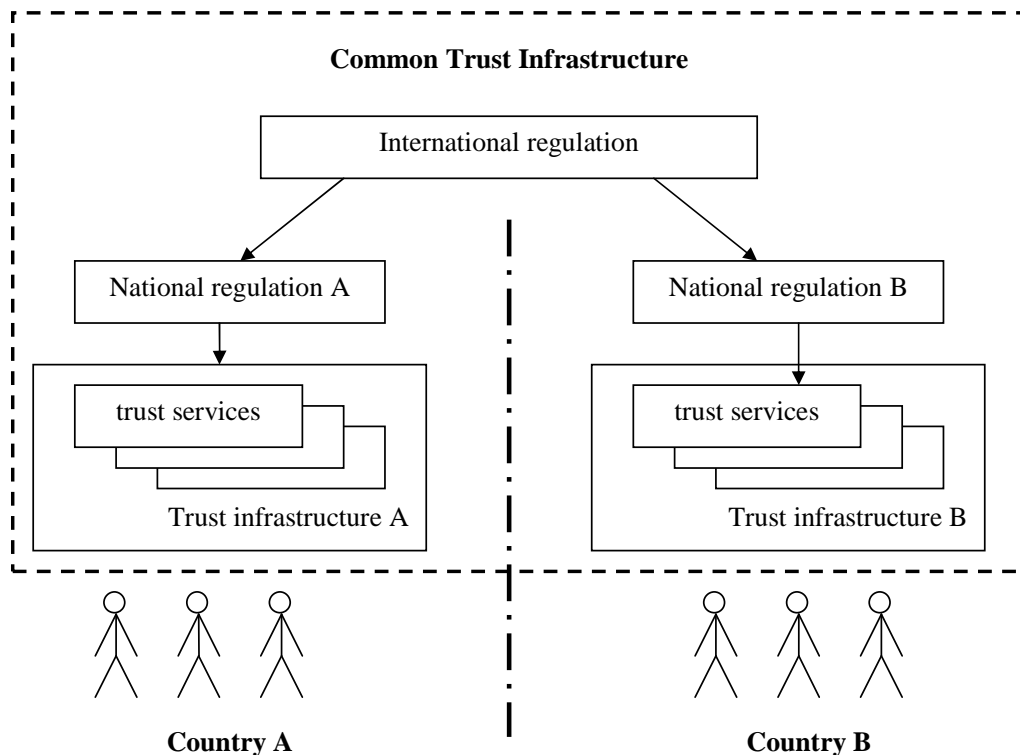
162

#### 163 **Legal level**

164 The CTI can be built on a single- or multi-domain basis. In the context of legal and  
165 organizational regulation, the multi-domain basis is the most complicated variant. Fig. 1 gives  
166 a general scheme of a legal regulation.

167

**Примечание [s1]:** From the  
project proposal



**Fig.1. Legal level**

168  
169  
170

171 Legal regulation of CTI interaction can be divided in two parts: international and national.  
172 The international legal regulation is carried out on the basis of the following types of  
173 documents:

- 174 – international treaties/agreements;
- 175 – acts of different international organizations;
- 176 – international standards and regulations;
- 177 – agreements between participants of transboundary information interaction on given issues;
- 178 – model acts.

179

180 The national legal regulation is built on a complex of normative documents that are standard  
181 in each particular jurisdiction.

182

183 We recommend a tight cooperation with UNCITRAL in order to harmonize the effort of this  
184 Recommendation concerning the necessary coordination on the legal level, see sec. 2.6.

185

### 186 **Organizational level**

187

188 Mutual legally significant recognition of trust services provided under jurisdiction of various  
189 states is reached through creation and operation of the dedicated body (let call it International  
190 Coordination Body or ICB) that includes national regulation bodies. The activity of ICB is  
191 regulated by the ICB Statute which is to be recognized and signed by all its authorized  
192 members – that is the Regulation Bodies of the Electronic Data Interchange represented  
193 primarily by the National Regulators of the CTI.

194

195 **Technological level**

196

197 There can be a great number of technological options for trust services' realization. The main  
198 requirement to the CTI elements is interoperability. Regulation at this level is carried out with  
199 application of different standards and instructions set forth by the ICB documents.

200

201 **2.4. Trust infrastructures services technical interoperability ensuring approaches**

202 *Identify approaches to ensuring interoperability of technical systems, infrastructures of trans-*  
203 *boundary electronic data exchange and end users including functional requirements and*  
204 *information security requirements.*

205 *Identify appropriate trust services types provided by the trusted infrastructures for ensuring*  
206 *legally significant trans boundary electronic data exchange.*

Примечание [s2]: From project proposal

207 **2.5. Trust infrastructures services levels of trust**

208 *Identify the possible levels of trust afforded by the trusted infrastructures and mechanisms by*  
209 *which these levels can be provided. For example, lower levels of trust may not require*  
210 *government directives for achieving a legally significant electronic interaction. UN/CEFACT*  
211 *recognizes that guidance for required levels (possibly higher) of trust and for desired levels of*  
212 *authentication depends on specific circumstances but such guidance does not constitute the*  
213 *scope of this recommendation. For these different levels of trust identify:*

214 *- common set of requirements trust services must comply with. Such requirements are to cover*  
215 *the following aspects: security, accessibility, and interoperability*

216 *- best practices for trust services initiation, certification and audit procedures.*

Примечание [s3]: From project proposal

217 **2.6. Communication with organizations in different areas of standardization**

218 *Identification of international organizations in different areas of normative and legal*  
219 *regulation and policies (such as WTO, UNCITRAL, WCO and others) for participation in the*  
220 *defining conditions for establishing necessary level of trust between the participants of the*  
221 *trusted infrastructure that will ensure legal significance of transboundary electronic*  
222 *exchange of data issued in different jurisdictions.*

223 *Identification of international organizations in different areas of standardization (such as*  
224 *ISO, W3C, ETSI and others) for participation in all the technical aspects of forming and*  
225 *functioning transboundary trust space.*

Примечание [s4]: From project proposal

226



### 227 3. ANNEX 1

#### 228 Terms and Definitions<sup>3</sup>

##### 229 *authentication*

230 – Anders Tornqvist: means an electronic process that allows the **confirmation** of the  
231 electronic identification of a natural or legal person; or of the origin and integrity of an  
232 electronic **data**.

Примечание [AN5]: I agree.

233 – Igor Furgel: a process of the verification of *authenticity*. A successful *authentication*  
234 (along with other factors) can be a necessary condition for the determination of the *legal*  
235 *validity* (of an *entity*).

236 – Eric E Cohen ([http://www.isaca.org/Knowledge-](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)  
237 [Center/Documents/Glossary/glossary.pdf](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)):

Код поля изменен

238 1. The act of verifying identity (i.e., user, system)

239 Scope Note: Risk: Can also refer to the verification of the correctness of a piece of data

240 2. The act of verifying the identity of a user and the user's eligibility to access  
241 computerized information

242 Scope Note: Assurance: Authentication is designed to protect against fraudulent logon  
243 activity. It can also refer to the verification of the correctness of a piece of data.

Примечание [IF6]: This is  
,authorization', but not  
,authentication', see below

244 – Ramachandran: the process of validating the identity of someone or something. Generally  
245 authentication requires the presentation of credentials or items of value to really prove the  
246 claim of who you are. The items of value or credential are based on several unique factors  
247 that show something you know, something you have, or something you are.

248 A process used to confirm the identity of a person or to prove the integrity of specific  
249 information. Message authentication involves determining its source and verifying that it  
250 has not been modified or replaced in transit.

251

##### 252 *authenticity*

253 – Anders Tornqvist: means that the **data** can be checked for its **authenticity** in a certain  
254 context.

Примечание [AN7]: –Cf the  
VAT Directive 2010/45 where in  
relation to the "authenticity" of an  
invoice the following is  
commented: "The supplier must be  
able to provide assurance that the  
invoice was indeed issued by him  
or in his name and on his behalf."  
–

255 – Igor Furgel: the property of an entity to evidence the identity of its issuer.

256 – Ramachandran:

Примечание [IF8]: ,authentic  
ity' is defined by using  
,authenticity'; it is a dead loop.

257 1. The *authenticity* is an auditable process that ensures a high level of quality in the  
258 results by maintaining evidence of trustworthiness of the identity and integrity of data  
259 messages

260 2. *Authenticity* is the status of being dependable in regard to evidence of identity and  
261 integrity in accordance with the agreed level of assurance.

<sup>3</sup> *Italic face* tags the terms defined in the current Recommendation

- 262 3. *Authenticity* is generally understood in law to refer to the genuineness of a document  
263 or record, that is, that the document is the “original” support of the information it  
264 contains, in the form it was recorded and without any alteration.” Authenticity is the  
265 property of being genuine and able to be verified and trusted.  
266 4. *Authenticity* in the electronic environment, further to the high levels of identification,  
267 evidentiary and attribution functions may be able to be established through an  
268 “authentication framework.” This “authentication framework” would involve legal  
269 infrastructure, some technical infrastructure and some organizational infrastructure.

270

271 ***authorization (as a process)***

- 272 – **Eric E Cohen**: the approval, permission, or empowerment for someone or something to do  
273 something.  
274 – **Igor Furgel**: approving a subject (a person, an IT component or a process acting on behalf  
275 of them) for the execution of a certain action.

276 ***certificate***

- 277 – **Jari Salo** (<http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf>):  
278 means a data message or other record confirming the link between a *signatory* and  
279 signature creation data.

280 ***data unit***

281 a set of digits or characters treated as a whole.

282 ***digital certificate***

- 283 – **Aleksandr Sazonov**: means a data message or other record confirming the link between a  
284 public key (validation data) to a particular distinguished name in the X.500 tradition.  
285 – **Igor Furgel**: means an electronic attestation which links signature validation data of an  
286 entity to the entity and confirms the identity of that entity.

287 ***digital signature***

- 288 – **Eric E Cohen** ([http://www.isaca.org/Knowledge-](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)  
289 [Center/Documents/Glossary/glossary.pdf](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)):  
290 A piece of information, a digitized form of signature, that provides sender authenticity,  
291 message integrity and non-repudiation.  
292 A digital signature is generated using the sender’s private key or applying a one-way hash  
293 function.  
294 – **Igor Furgel** (ISO 7498-2 (1989): ‘Information processing systems - Open Systems  
295 Interconnection - Basic Reference Model - Part 2: Security Architecture’):  
296 Data appended to, or a cryptographic transformation of, a *data unit* that allows a recipient  
297 of the *data unit* to prove the source and integrity of the *data unit* and protect against  
298 forgery, e.g. by the recipient.

**Примечание [s9]:** **Eric E Cohen** This is in contrast to when you care not whether the agent is authorized, only that they are who they say they are - authentication. The two are usually considered orthogonal; you normally only wish to check one or the other. I believe in transboundary efforts, authorization is more important than authentication.

Код поля изменен

Код поля изменен

299 – Ramachandran: a *digital signature* is made when the owner of a key pair uses its private  
300 key to "sign" a message. This signature can only be verified by the corresponding key.

301 **electronic signature**

302 – Anders Tornqvist & DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT  
303 AND OF THE COUNCIL of 13 December 1999 on a Community framework for  
304 electronic signatures: means data in electronic form which are attached to or logically  
305 associated with other electronic data and which serve as a method of authentication.

306 – Eric E Cohen ([http://www.isaca.org/Knowledge-](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)  
307 [Center/Documents/Glossary/glossary.pdf](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)):

308 Any technique designed to provide the electronic equivalent of a handwritten signature to  
309 demonstrate the origin and integrity of specific data.

310 Digital signatures are an example of electronic signatures.

311 – Igor Furgel:

312 data in electronic form which are attached to or logically associated with other electronic  
313 data. *Electronic signature* documents a relationship between the *signatory* and these other  
314 electronic data and enables (also) a third party to subsequently ascertain this relationship.

315 – Jari Salo (<http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf>):

316 data in electronic form in, affixed to or logically associated with, a data message, which  
317 may be used to identify the signatory in relation to the data message and to indicate the  
318 signatory's approval of the information contained in the data message.

319 – Ramachandran: Data in electronic form in, affixed to or logically associated with, a data  
320 message, which may be used to identify the signatory in relation to the data message and  
321 to indicate the signatory's intention in respect of the information contained in the data  
322 message. An electronic signature should not be discriminated because of its origin. But  
323 may be discriminated because of their intrinsic qualities

324  
325 **entity**

326 – Igor Furgel: can be a document, a record, an identifier etc (generally: a *data unit*).

327 **genuineness (in IT)**

328 – Igor Furgel: *integrity* + *authenticity* = the property of an *entity* to evidence:

329 (a) not having been altered from that created by its issuer

330 AND

331 (b) the identity of its issuer.

332 – Ramachandran: the quality that ensure document's property of being genuine.

333 **genuineness (in law)**

334 – Igor Furgel: ([130201+Rec14+survey+on+def\\_levels+consolidated+responses](#)):

335 "Authenticity is generally understood in law to refer to the *genuineness* of a document or  
336 record, that is, that the document is the "original" support of the information it contains, in

**Примечание [IF10]:** This definition is not a full one, there are also other services of electronic signature.

The main services of a signature are (i) perpetuation function (a signature can be verified by anybody later on at any time), (ii) the determinability of the identity of signatory. Additionally, there are warning and consciousness functions.

**Код поля изменен**

**Примечание [IF11]:** There is a quite controversial discussion on it.

**Код поля изменен**

**Примечание [IF12]:** Not unconditionally an approval, but, generally, a relationship between the signatory and the message

**Примечание [AN13]:** The UNCITRAL definition is not uncontroversial. We should also look at the new definitions of e-signature and e-seal of the EU EIDAS Regulation, rather than the -99 Directive referenced above.

**Примечание [IF14]:** The footnote No. 5 in the REC. 14 may also be helpful here:

"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. "

337 the form it was recorded and without any alteration.” *Authenticity* is the property of being  
338 *genuine* and *able to be verified and trusted*”.

339 ‘*Genuineness*’ in law is equivalent to ‘*authenticity*’.

#### 340 *information interaction*

341 – Igor Furgel: the interchange of any data between the participants of interaction

#### 342 *integrity*

343 – Igor Furgel: the property of an *entity* to evidence **not having been altered from that**  
344 **created by its issuer**.

345 – Eric E Cohen ([http://www.isaca.org/Knowledge-](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)  
346 [Center/Documents/Glossary/glossary.pdf](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)):

Код поля изменен

347 **Guarding against** improper information modification or destruction, and includes ensuring  
348 information non-repudiation and authenticity.

Примечание [AN15]: Perhaps not always “guarding against” but rather allowing for detection of change.

349 – Ramachandran:

- 350 1. *DATA INTEGRITY*—A condition in which data has not been altered or destroyed in an  
351 unauthorized manner
- 352 2. *Integrity* is a state of information that assure that it is accurate, complete, consistent  
353 and has been protected from errors or unauthorized modification.
- 354 3. *integrity* refers to the resource is untampered with, uncorrupted and complete in all  
355 its essential respects after the act of signature is carried out.

#### 356 *levels of access*

357 – Igor Furgel: permission for a subject (a person, an IT component or a process acting on  
358 behalf of them) to get a specified kind of access (e.g. write, read, etc.) to specified objects  
359 (e.g. data, processes, information, other resources).

360 A successful *authentication* (along with other factors) can be a necessary condition for  
361 granting a certain *access level*. The terms ‘access level’ and ‘authorization level’ are used  
362 as synonyms in the context of the current Recommendation.

#### 364 *levels of authentication*

365 – Aleksandr Sazonov: a synonym for *levels of qualification of authentication service*.

367 – Ramachandran: a guidance concerning control technologies, processes, and management  
368 activities, as well as assurance criteria that should be used to mitigate authentication  
369 threats in order to achieve the required level of security based on the sensitivity of data or  
370 a service.

#### 371 *non-repudiation*

372 – Eric E Cohen: the ability for a system to prove that a specific user and only that specific  
373 user sent a message and that it hasn’t been modified. A user cannot deny/repudiate that  
374 they signed/sent a message.

375 **privacy**  
376 – Eric E Cohen ([http://www.isaca.org/Knowledge-](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)  
377 [Center/Documents/Glossary/glossary.pdf](http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf)):

Примечание [AN16]: Should we deal with “privacy” or “personal data” rather?

Код поля изменен

378 Freedom from unauthorized intrusion or disclosure of information about an individual and  
379 an organization.

Примечание [s17]: Eric E Cohen My *personal* interpretation includes information about both individuals (people) and organizations.

### 380 **signatory**

381 – Jari Salo (<http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf>):  
382 a person that holds signature creation data and acts either on its own behalf or on behalf of the  
383 person it represents.  
384 – Igor Furgel (Proposal for a Regulation of the European Parliament and of the Council on  
385 electronic identification and trust services for electronic transactions):  
386 a natural person who creates an *electronic signature*.

Код поля изменен

Примечание [IF18]: Not just acts, but creates an electronic signature

Примечание [AN19]: Possibly only “creates”, not necessarily “acts on behalf”.

Удалено: *stamping*

### 387 **time stamp**

388 – Eric E Cohen: a trusted indication of when an action, particularly the application of a  
389 digital signature, took place.  
390 – Igor Furgel (Proposal for a Regulation of the European Parliament and of the Council on  
391 electronic identification and trust services for electronic transactions):  
392 data in electronic form which binds other electronic data to a particular time establishing  
393 evidence that these data existed at that time.

Примечание [s20]: Eric E Cohen Time stamping is vital in cryptography as people change roles and signatures expire; it is important to know whether the signature was valid and the signer was authorized or could be authenticated at the point of *signing* rather than the point of *checking*.

### 394 **transboundary trust space**

395 – Aleksandr Sazonov: a set of normative, organizational and technical conditions for  
396 establishing trust in transboundary electronic interaction between public governmental  
397 authorities, public non-budgetary funds, local authorities, organizations and citizens.  
398 – Ramachandran: a technological and legal framework for trust establishment in  
399 transboundary electronic informational interaction of entities in different legal  
400 frameworks’ subjects.  
401 – Eurasian Economic Community Agreement: an aggregate of legal, organizational and  
402 technical conditions, harmonized by the member-states in order to ensure trust in  
403 international exchange of data and electronic documents between authorized bodies.

### 404 **trust domain**

405 – Igor Furgel: informational and legal space using the same CTI

### 406 **what-you-see-is-what-you-sign**

407 – Aleksandr Sazonov: is a desirable property of electronic signature systems meaning that  
408 the semantic interpretation of a electronically signed message cannot be changed, either  
409 by accident or by intent.

410 *XML Signature*

411