United Nations ECE/TRADE/C/CEFACT/2018/7

Economic and Social Council

Distr.: General
13 February 2018

Original: English

Economic Commission for Europe

UNECE Executive Committee

Centre for Trade Facilitation and Electronic Business

Twenty-fourth session
Geneva, 30 April and 1 May 2018
Item 7(b) of the provisional agenda
Recommendations and standards: Other deliverables for noting

White Paper on Trusted Transboundary Environment

Ensuring Legally Significant Trusted Trans-Boundary Electronic Interaction

Summary

When exchanging information electronically, there can be questions of the legal significance of the data, in other words, if the information received is legally binding. Building on the work of UNECE Recommendation 14 on Authentication of Trade Documents, this White Paper aims to provide guidance on establishing a mutual recognition framework between countries in view of ensuring the legal significance of information, when higher levels of reliability are required or are desired. This is the Trusted Transboundary Environment. This work can eventually form the basis of future work on the subject.

This document is submitted to the twenty-fourth Plenary for noting.

GE.18-02195(E)
1802195

I. Introduction

1. The intention of this paper is to facilitate and encourage the creation of a trusted transboundary environment for the international legally significant exchange of electronic documents and data between public authorities, and natural and/or legal persons. This paper is intended for those parties interested in the establishment, operation and practical usage of such transboundary infrastructures.

2. The Internet has become a habitual tool and environment for obtaining electronic services for individuals and entities of various states. The advantages of such services are evident, but a number of organizational and legal issues prevent their widespread use in cases where parties require a certain degree of confidence in each other, and in the electronic services they use. One of the main issues is ensuring the legal validity of e-documents and the legal significance of electronic interaction in general. This problem is urgent on both the national level (within single jurisdictions) and the transboundary level (where interactions occur between participants acting under the jurisdiction of different states).

3. The following scenarios represent some examples where a certain *degree of confidence* is required:

- Electronic tendering procedures, especially the cases where the contracting authority is a governmental body or a big company. These authorities usually require a higher level of reliability for the trade documents of their economic operators.
- Certain trade and transport documents exchanged within cross-border trade procedures.
- Dispute resolution and settlement procedures including online dispute resolution. These procedures require the univocal identification and authentication of a plaintiff and defendant.
- Electronic insurance. There should be a mechanism for the reliable verification of an insurance certificate

4. The urgency of establishing national environments for paperless trade is mentioned in some regional arrangements for the facilitation of cross-border paperless trade such as the Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific issued by the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP). One of the purposes of this White Paper is to support Governments, and regional and international organizations in building up and managing these environments in an interoperable way.

5. As stated in Recommendation 14, UN/CEFACT advocates the removal of any excessive rulings, contracts or practices (when possible) to facilitate international trade procedures. Nevertheless, there remain trade-related scenarios where participants seek a high *degree of confidence* in each other. This White Paper facilitates exactly such scenarios.

6. This White Paper explores the principles of establishing and operating regional and global coordination organizations which ensure trust in the international exchange of data and electronic documents between participants interacting within an electronic framework (i.e. public authorities, and natural and legal persons).

7. This White Paper covers mainly organizational, and partially technological, provisions concerning trusted Information and Communication Technologies (ICT)

services. Provisions regarding the establishment of appropriate legal regimes may be elaborated by other bodies.

8. The general purpose of this White Paper is to help ensure the rights and legal interests of citizens and organizations while they perform *legally significant*[1] information transactions in electronic form, using the Internet and other open ICT systems of mass usage.

9. In order to achieve a higher *degree of confidence* in electronic interaction, this White Paper explores the establishment of a *Common Trust Infrastructure (CTI)*—a fundamental, easily scalable platform that includes dedicated, trusted ICT services and provides unified access to these services.

10. UN/CEFACT recognizes the principle of technological neutrality and does not propose any specific technology as a basis for a *CTI*. It is up to governments to choose the technologies which will provide the necessary *degree of confidence* in the electronic interaction. This White Paper focuses on organizational aspects of *CTI* and elaborates technical issues merely to the extent necessary for making the approaches applicable in practice.

II. Basic principle of Common Trust Infrastructure

11. Participants in electronic interactions typically deal with some kind of ICT service (email, cloud storage, web-portals, etc.). If such participants already have a sufficient *degree of confidence* in each other and in the ICT services they use, then nothing needs to be changed. But if the participants are not sufficiently confident in each other and/or in the ICT services they are using, then it may be appropriate to use a trusted third party to help increase the *degree of confidence* in the electronic interaction. The services provided by these trusted third parties are called *trust services.*

12. Within this White Paper, *trust services* may be of different types (provide different functions) and of different *levels of qualification*. *High level qualification trust services* are operated under one or more international agreements, and they meet the requirements and follow the rules laid out by international coordinators. *Basic level qualification trust services* are operated under one or more commercial agreements, and they may be established within, for example, some large scale international projects and follow the recognized best practices for trust service providers. *Trust services* should be audited in accordance with their *level of qualification.*

13. The aggregate of *trust services* operating within the legal, organizational and technical framework forms the *Common Trust Infrastructure*. The *CTI* is a fundamental, easily scalable infrastructure platform providing unified access to *trust services*.

14. The existing natural peculiarities of different world regions (historical, cultural, political, economic, technical, etc.) may result in different *levels of trust* within these regions concerning electronic interactions.

15. The primary objective of a *CTI* is to ensure *legally significant* electronic interactions between its users by providing *trust services* of different *qualifications* (zero, basic, high) to the participants of an electronic interaction.

[1] Attaching the attribute “legally significant” to an electronic interaction will require a legal framework that is outside the scope of this White Paper.

16. This institutional guarantee is to be ensured within the business activity of specialized providers which:

- provide users with a set of trusted ICT services;
- operate within established legal regimes, which include but are not limited to restrictions imposed by the processing of personal data; and
- operate within the context of a Common Trust Infrastructure.

III. *Common Trust Infrastructure* establishment principles

- **Scalability**. The CTI should be established in such a way that it can be easily scaled. It broadens easily at any level of consideration due to the accession of new participants, such as new jurisdictions; new supranational participants; new providers of trust services, and register systems.
- **Traceability**. If required by the participants of electronic interaction, any fact of electronic interaction within the CTI should be recorded and available for conflict resolutions if necessary.
- **Cost efficiency**. While deciding on a concrete variant of CTI architecture, the risk analysis should be taken into account. The CTI forming and functioning costs should be lower than possible losses caused by ICT-specific malfunctions and malicious activities.
- **Complexity**. Coherent elaboration of legal, organizational and technological issues should be performed during the establishment of a CTI. A complex description allows for the correct functioning of the system as a whole, and its single elements.

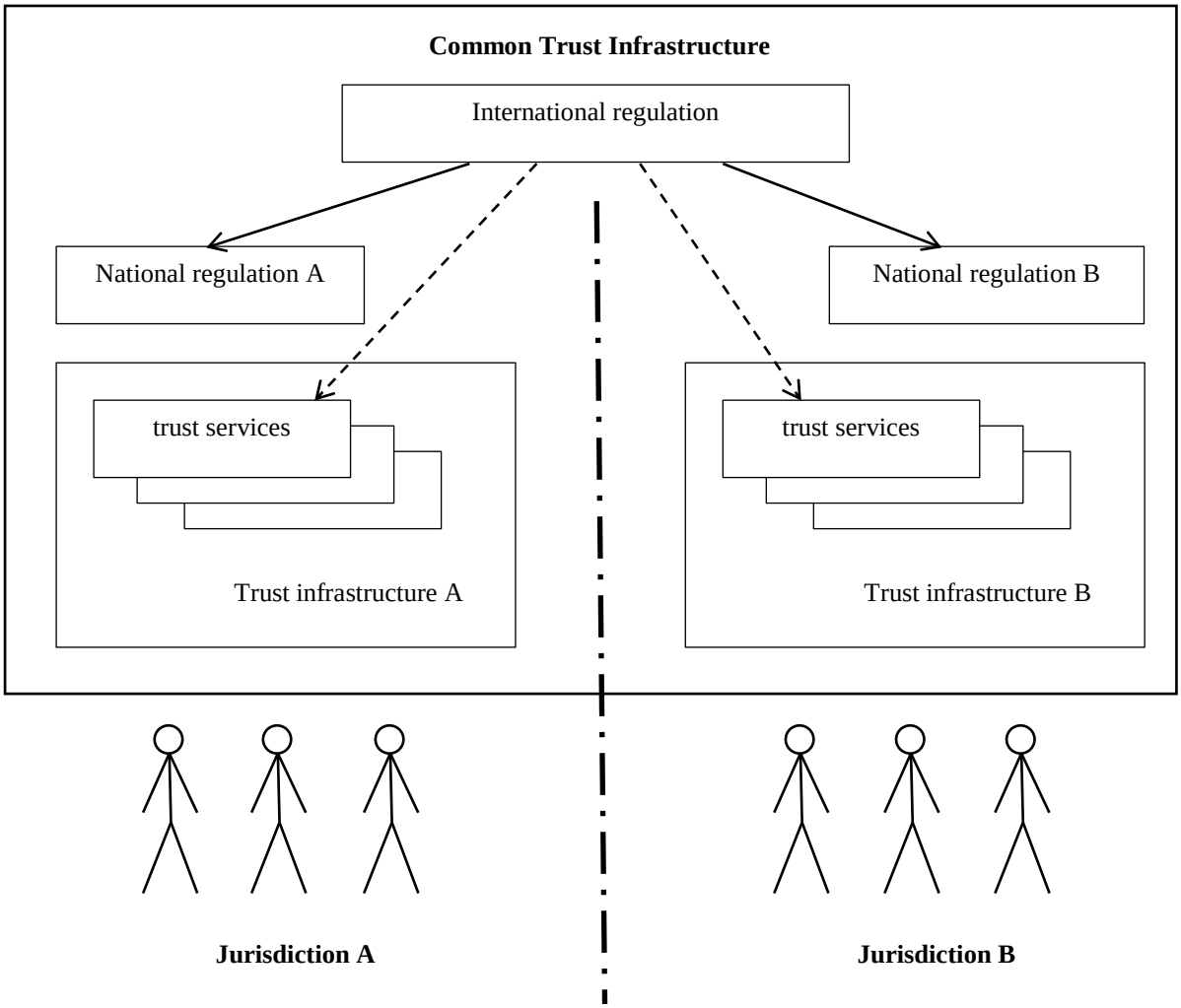
IV. *Common Trust Infrastructure* coordination approaches

17. The *CTI* architecture is selected according to the principles stated in the previous section. There are three levels of *CTI* coordination: legal, organizational and technological.

A. Legal Level

18. The *CTI* can be built on a single- or multi-*domain* basis. In the context of legal and organizational regulation, the multi-*domain* basis is the most complicated variant. Fig. 1 gives a general scheme of a possible approach to legal regulation. The dotted arrows depict the cases where a national regulation does not exist, or where it is not feasible.

Fig.1. Legal level



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

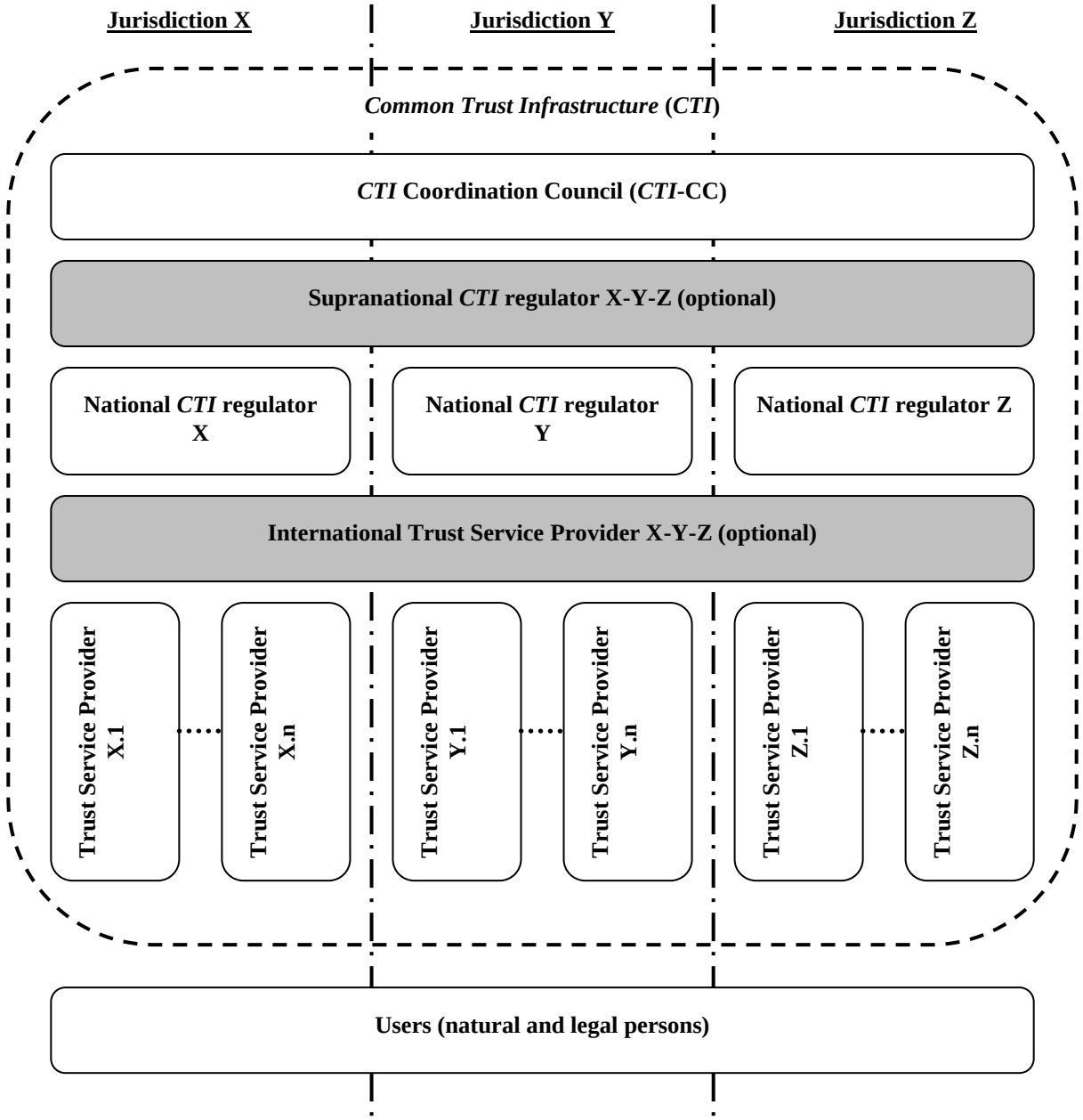
- international treaties/agreements;
- acts of different international organizations;
- international standards and regulations;
- agreements between participants of transboundary electronic interaction on given issues;
- model acts.

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

B. Organizational Level

21. Mutual *legally significant* recognition of electronic documents and data treated by *trust services* provided under various jurisdictions could be reached through the creation and operation of a dedicated body (in this example called a *CTI* Coordination Council or *CTI*-CC) that includes national regulation bodies having voluntarily joined the *CTI*-CC. The activity of *CTI*-CC could be regulated by a *CTI*-CC Statute which should be recognized and signed by all its authorized members – that is the Regulation Bodies of the Electronic Data Exchange represented primarily by the National *CTI* Regulators. Fig. 2 gives a general scheme of the organizational level of coordination. The optional elements are identified by grey blocks.

Fig.2. Organizational level



22. The *CTI*-CC issues a number of documents interconnected with its Statute:

- **Requirements** for the CTI-CC members, compliance is a prerequisite for full membership in the CTI-CC;
- **Guidelines** for carrying out 'shadow' supervision for admittance to the CTI-CC and periodic mutual audit for maintaining voluntary membership in the CTI-CC;
- **Compliance criteria** which are to be met by providers of the trust services, and the methodology for applying these criteria;
- **Scheme of estimation/verification** of providers of the trust services with respect to their meeting these criteria.

23. In the *CTI*, each jurisdiction is represented by a National *CTI* regulator (see Fig. 2) which regulates the activity of providers of the *trust services* within its jurisdiction.

24. For groups of member states with a high degree of integration (for example, Eurasian Economic Union member-states or European Union member-states) there is a possibility of constituting a Supranational *CTI* regulator (Fig. 2, Supranational *CTI* regulator X-Y-Z). In such case, one Supranational *CTI* regulator X-Y-Z substitutes for a group of National *CTI* regulators X, Y and Z.

25. The natural *CTI* scalability is enabled through the procedure for admitting new members to the *CTI*-CC (new national and supranational participants) and the scheme for verifying that the providers of the *trust services* meet the *Compliance criteria* issued by the *CTI*-CC (new providers of the *trust services*).

26. International providers of *trust services* can provide, inter alia, neutral inter-domain gateways as a specific type of *trust service*. The main function of an inter-domain gateway is to provide for mutual recognition (legalization) of electronic documents and data. These inter-domain gateways connecting single *domains* represent the elements in building a *CTI*.

27. Inter-domain gateways can be established simply, at the legal and organizational levels; and at a complex level (legal, organizational and technical).

28. In the first case, the communicating *domains* establish a common legal basis for cooperation between them (see 'Legal level' section above). This legal basis defines the full set of requirements, conditions and prerequisites, enabling and even guaranteeing a mutual legal recognition (legalization) of *legally significant* electronic documents.

29. On the organizational level, procedures and processes of interaction between different *domains* shall uphold the *level of trust* between these *domains* as being sufficient for a mutual recognition (legalization) of electronic documents and data issued in different *domains* or jurisdictions.

30. In order to achieve this necessary *level of trust*, this set of the requirements, conditions and prerequisites shall regulate, inter alia, the establishment and operation of a neutral international environment, i.e. an environment outside (beyond) any single *domain*. The *CTI*-CC and International trust service providers represent parts of this neutral international environment. Such a neutral international environment could be operated in a neutral legal field that is defined by an international body.

31. In a situation where inter-domain gateways are established at only legal and organizational levels, these inter-domain gateways are implemented merely by treaties, agreements and organizational procedures. This legal and organizational infrastructure may be supported by different single *trust services* like e-signature verification, powers verification, time stamping etc., but without a specific *trust service* dedicated to the purpose of being a gateway.

32. In the second (complex) case, when inter-domain gateways are established at legal, organizational and technical levels, inter-domain gateways additionally transform a document in such a way that it will fulfil the requirements (attributes, format, structure, etc.) for *legally significant* electronic documents in a recipient's *domain*[2] (jurisdiction). In this way, the inter-domain gateway *trust service* can substitute for a number of *trust services* that provide only single specific functions (e-signature verification, powers verification, time stamping etc.). As ever, technically implemented inter-domain gateway *trust services* shall also be operated in a neutral international environment.

33. Approaches to forming inter-domain gateways should consider the usage of transition profiles describing and configuring transitions from one *domain* to another. These transition profiles should take into account, inter alia, the legal basis of the cooperation between the communicating *domains* as well as the *levels of qualification* of the identification schemes used inside the interacting *domains*.

34. In order to become a National Trust Service Provider, a supplier of these services should undergo accreditation with the National *CTI* regulator of the same jurisdiction. International Trust Service Providers should undergo accreditation with the *CTI*-CC. The requirements for accreditation of the providers of the *trust services*, and the requirements of their activity, should be regulated by the compliance criteria issued by the *CTI*-CC, and possible national supplements issued by the respective National *CTI* regulator.

35. In the *CTI*-CC, the users of electronic services could be both individuals and legal entities. The users select the necessary *level of qualification* of a *trust service* at their discretion, or in an agreement.

36. The services should be provided by the respective suppliers—the *trust service* providers. The *trust service* providers should be integrated by the *CTI*.

37. The *trust services*, as the *CTI* elements, could be variously realized depending on the *level of trust* between *domains* (jurisdictions). For example, with a conditionally ‘high’ or ‘medium’ level of mutual trust between the *CTI* members, it is efficient to use centralized International *trust services* applied according to agreed-upon standards. In the case of a conditionally ‘low’ *level of trust*, the *trust services* are built according to the decentralized principle—national *trust services* in each single jurisdiction.

C. Technological level

38. There can be a great number of technological options for *trust services*’ realization. The main requirement of the *CTI* elements is interoperability. Regulation at this level is carried out by the application of different standards and instructions set forth by the *CTI*-CC documents.

39. This White Paper recommends close cooperation with major technical standardization organizations such as ISO, ETSI, W3C, CEN and others in order to achieve the necessary coordination on the technological level[3].

[2] 'Domain' or 'trust domain' can coincide with a single jurisdiction or can unite several jurisdictions

[3] International Organization for Standardization (ISO), European Telecommunications Standards Institute (ETSI), World Wide Web Consortium (W3C), European Committee for Standardization (CEN)

V. Trust infrastructures services: approaches to ensure technical interoperability

40. To determine *trust services* types it is advisable to consider whether a base document's attributes are necessary to fulfil the document's legal function.

Table 1: document's attributes necessary to fulfil its legal function

No.	Attribute type	Mandatory yes/no	Description / comments
1.	Content	yes	An aggregate of at least one of the following attributes is the content—the informational essence of a document irrespective of form (i.e. paper or electronic): 1) document type 2) document classification 3) document title 4) table of contents 5) document body (mandatory) 6) annexes Herewith, information integrity and authenticity are to be assured when processing, storing and transferring.
2.	Document issuer legal status	yes	An aggregate of the following attributes is the document issuer legal status: 1) logo type 2) name of an issuer 3) issuer reference data (address, contacts etc.) 4) seal impression
3.	Signatory status (powers) or signatory position	no	A brief description of signatory powers with their duration stated.
4.	Signature	yes	An aggregate of the following attributes is the signature: 1) issuer‘s signature 2) signature stamp of confirmation 3) signature stamp of approval 4) visa (clearance / endorsement stamp) 5) copy certification stamp 6) seal of issuing organization 7) etc.
5.	Time	yes	A statement of the time of signing, attached on the basis of a trusted time source (the validity aspect).
6.	Place	no	A statement of the place of signing (the place where the Signatory expressed his/her will to sign by triggering signing) is optional. If this type of service is not available, the attribute place can be considered as one of the content attributes.

41. Basic *trust services* types (trust services functions provided depending on concrete demand) are:

a. Creation, verification, and validation of signatures and seals

b. Monitoring of legal status

c. Creation, verification, and validation of time stamps

d. Providing neutral inter-domain gateways

Note: If there is a gateway between domains (jurisdictions), there should be a profile for this inter-domain gateway based on an agreement between these domains. Each inter-domain gateway profile should "know" what attributes are mandatory for each domain. On the technological level, an inter-domain gateway should implement some protocol translation or translation of different protocols or standards from one domain to another. For the mathematical description of inter-domain gateway functions please refer to Annex 2. Trust services (including inter-domain gateways) work with national identification schemes on the one hand, and with international trust infrastructure (other trust services) on the other.

e. Providing identification of natural and legal persons

42. The following attribute types (see Table 1) presume a previously performed identification of related natural or legal persons:

- document issuer legal status
- signatory status (powers) or signatory position
- Signature

43. The *trust service* types a) and b) use these attribute types and, hence, also presume a previously performed identification of related natural or legal persons. The identification services are provided by providers specialized in performing identification. These services can be implemented on different *qualification levels*: zero, basic and high. The *CTI*-CC shall decide/agree upon eligible identification schemes, including minimal requirements on them. There may be *CTI*-CC specific identification schemes and/or references to international standards and/or references to notified identification schemes inside a single *domain.*

44. Sets of identification attributes and identification procedures themselves can serve as the basis for the definition of the *qualification levels* of identification schemes. The *qualification levels* of identification schemes can be of essence for the regulation of interaction between different *domains*. Sets of identification attributes can be defined by the legal regimes for the business activity of providers specialized in performing identification and of functional providers. Sets of identification attributes can be maintained by the *trust services* (identification service). The activity of providers specialized in performing identification can be regulated by special organizational and technical requirements created to ensure personal data protection.

45. Note: Long-term archival and related verification services can be realized as a function of ICT service or as a function of a special trust service type.

46. Note: Existing electronic systems should be taken into account so that requirements for their updating and connection to the *CTI* may be minimal.

VI. Common Trust Infrastructure services levels of qualification

47. The *level of qualification* of a *trust service* is a function of the trust service to evidently fulfil a predefined set of requirements.

48. There can be distinct incremental *qualification levels* of a *trust service*. The lower the degree of confidence of the participants in each other and in the ICT services

processing electronic interactions (i.e. creation, access, transformation, transmission, destruction, etc.), the higher the demand on the *qualification level* of *trust services.*

49. The characteristics of the *levels of qualification* of *trust services* are described in the following table.

Table 2: characteristics of the levels of qualification of trust services

	Degree of confidence participants have in each other and in the ICT services		
	High degree of confidence	**Substantial degree of confidence**	**Limited degree of confidence**
levels of qualification of trust services	No trust services required ('zero' level of qualification)	Basic level of qualification	High level of qualification
legal regime of operation of trust services	n/a	Based on commercial agreements and/or common trade practice	Based on international agreements (conventions) and/or on directly applicable international regulation[4]
Organizational architecture of trust services	n/a	Large Scale Projects of any kind	*CTI*- Coordination Council (*CTI*-CC), see Title IV above
Technological requirements on trust services	n/a	Meet the recognized best practices for trust service providers	-- Meet *CTI*-CC Compliance Criteria AND -- Meet the requirements laid down in the applicable national regulation (for national trust service providers)

50. If *trust services* engaged in document lifecycle (incl. the chain of inter-domain gateways between the document's issuer and recipient) have different *levels of qualification*, the overall *level of qualification* is equal to the lowest of them.

VII. Communication with organizations in different areas of standardization.

51. This White Paper suggests creating a description of different possible legal regimes:

- based on international agreements (conventions) and/or on directly applicable international regulation;
- based on commercial agreements and/or common trade practice;
- without special international regulation.

52. Legal regimes can be additionally supported by traditional institutes (governmental authorities, judicial settlement, risk insurances, notaries public and others) through mutual recognition of electronic documents secured by *trust services.*

[4] E.g. *trust services* operated in accordance with EU Regulation (eIDAS) or Eurasian Economic Union Agreement and other documents.

53. Established legal regimes can also be used to impose special requirements on the materials, and financial support of the business activity of specialized providers in case of damage to their users, including cases of compromised personal data.

54. Institutional guarantees and legal regimes for constituting and functioning regional and global transboundary trusted environments should be considered in a separate document by a specialized body

55. This paper suggests describing the mechanisms of interaction between particular states and their international unions with other international formats within the framework of creating a common transboundary trusted environment.

a. by means of the complete or a partial joining of a state to an existing legal regime on the basis of international treaties and/or directly applicable international regulations, in the context of which a task on forming a regional transboundary trusted environment has already been set or solved. This existing legal regime ensures institutional guarantees to the subjects of electronic interaction.

b. In the context of interaction between different international unions:

- In the first stage, a group of states creates a regional domain ensuring institutional guarantees for the subjects of electronic interaction within the legal regime specified by these states;
- In the second stage, the protocols of trusted interaction with other international unions are specified as related to mutual recognition of different legal regimes. This mutual recognition shall pertain to institutional guarantees and information security requirements concerning each of the international formats, possibly on the basis of an inter-domain gateway being operated within the framework of an international legal regime.

c. In the context interaction of a state with other states or international unions:

- In the first stage, a state creates its own domain functioning in the framework of a national legal regime specified by this state;
- In the second stage, the protocols of trusted interaction with other states and/or international unions are specified as related to mutual recognition of different legal regimes. This mutual recognition shall take in account institutional guarantees and information security requirements pertaining to these states and international formats, possibly on the basis of an inter-domain gateway being operated within the framework of an international legal regime.

VIII. Communication with international organizations in different areas of standardization on the technical and organizational aspects of forming a functioning transboundary trusted environment

56. This White Paper suggests taking into consideration the following aspects of standardization:

Technological Aspects

57. The main objective of standardization in this area is facilitating technical interoperability within the transboundary trusted environment. This should cover all technical aspects that necessarily impact functional and security interoperability like documents and data formats, communication protocols, format and protocol conversions,

technical interfaces, the equivalence of the assurance (security) level of technical components, etc.

Organizational Aspects

58. The main objective of standardization in this area is to support a *level of trust* between domains as being sufficient for a mutual recognition (legalization) of electronic documents and data, which are issued in different *domains* (jurisdictions). This includes, but is not limited to, procedures for performing conformity audits of *trust service* providers by independent conformity assessment bodies; for accrediting these conformity assessment bodies; for mutual "peer-to-peer" audits between the members of the *CTI* Coordination Council, objects and areas subjected to the audits and the applicable audit criteria.

59. The specified aspects should be considered as they are applied to different *levels of qualification* of *trust services*. If a *trust service* with a lower *level of qualification* interacts with a *trust service* with a higher *level of qualification*, the whole *level of qualification* of the interaction between both *trust services* will be, at most, equal to the lower *level of qualification.*

Annex I

Glossary

Italic face indicates the terms defined for the purposes of this White Paper.

For the purposes of this paper the following terms apply:

- ***Common Trust Infrastructure (CTI)***
  - An infrastructure designed to help ensure the *legal significance* of transboundary electronic interaction. *CTI* provides a set of *trust services* harmonized on the legal, organizational and technological levels.
- ***Degree of confidence*** (of the participants of electronic interaction in each other and in the ICT services processing the electronic interaction between them)
  - A societal function of an established or felt degree of confidence of the participants of electronic interaction in each other and in the ICT services processing the electronic interaction between them.
- ***Legal significance*** (of an action)
  - A property of an action (of a process) to originate (to result in) documents (data units) possessing *legal validity*.
- ***Legal significance*** (of a document)
  - A property of a document (data unit) to change the legal status of a subject of law (a natural or legal person who in law has the capacity to realize rights and juridical duties).
  - A *legally significant* document is always also a *legally valid* one with concrete content.
- ***Legal validity (also called 'legal force')*** (of a document)
  - A property of a document (data unit) to be applicable for judicature, i.e. be deemed to have satisfied the requirements of applicable law. The *legal validity* is conferred to a document by the legislation in force, by the authority of its issuer and by the established order of its issuing (e.g. it shall be usable for a subsequent reference).
- ***Level of qualification*** (or qualification level) (of a service)
  - A property of a service to evidently fulfil a predefined set of requirements.
- ***Levels of trust*** (between domains)
  - A societal function determining the degree of trust between *domains*.
  - Depending on an established *level of trust*, *domains* are prepared to share a certain amount of resources and to jointly use certain infrastructures; i.e. *domains* are prepared to delegate part of their inherent powers, functions and resources to a *common trust infrastructure* (*CTI*), in which they jointly trust. The higher the *level of trust* in this *CTI* the more inherent powers *domains* are prepared to delegate to the *CTI*.
- ***Domain*** (trust domain)

- Informational and legal space using the same *CTI*. A *domain* can coincide with a single jurisdiction or can unite several jurisdictions.

- ***Trust service***
  - (high level definition) - an electronic service aiming to ensure a certain *degree of confidence* between the participants of an electronic interaction.

- ***Trusted electronic interaction***
  - The exchange of any data in electronic form in such a way that a user of this data undoubtedly accepts it according to its operational policy. Each user's operational policy determines whether the electronic interaction is considered a trusted one. Hence, the determination of the trustworthiness of data received in an electronic exchange varies from one user to another. Any electronic interaction utilizes information and communication technology services (such as an internet provider, email provider, message exchange services of any kind, cloud storages, etc.); however, *trusted electronic interaction* is provided by using *trust services*.

Annex II

Mathematical description of inter-domain gateway functions

The set of rules to translate the related requirements between two domains A and B should be laid down within an inter-domain gateway.

$A=\{a_1, a_2,..., a_N\}$

$B=\{b_1, b_2,..., b_M\}$

$E(a)=A \rightarrow B$

Where A is the set of requirements (attributes) for domain A, B is the set of requirements for domain B, and E(a) is the set of transformation rules from A to B. Keeping in mind that the power of the sets (i.e. the quantity of requirements) in a real-world scenario may not be equal ($N \neq M$), there should be rules defined to lead both sets to equal power K where K=MAX(N, M).

The degree of trust to this set of transformation rules can be defined as transformation to some universal superset of requirements, and such transformation is performed inside each domain.

$E(a)=A \rightarrow X$

$E(x)=X \rightarrow B$

Where X is a universal superset of requirements for A and B.