UNITED NATIONS
CENTRE FOR TRADE FACILITATION AND ELECTRONIC BUSINESS
(UN/CEFACT)

REGULATORY PROGRAMME DEVELOPMENT AREA
E-GOVERNMENT DOMAIN

Ensuring legally significant trusted trans-boundary electronic interaction

DRAFT

SOURCE: Project Team
ACTION: Version prepared by Bureau to be suggested as a White Paper

DATE: 16 October 2017
STATUS: **Draft v0.98**

Foreword

~~This Recommendation is intended to help facilitate and encourage constituting a transboundary trusted environment for the international *legally significant*[1] exchange of electronic documents and data between public authorities, natural and/or legal persons. This Recommendation may attract attention of an audience that is involved/interested in the establishment and operation as well as in the practical usage of such transboundary infrastructures.~~

~~Executive summary~~

The UN Centre for Trade Facilitation and e-Business (UN/CEFACT) is engaged to provide guidance and electronic business standards to streamline processes. This encompasses electronic data exchanges between parties (private sector and/or public sector). Though UN/CEFACT strives to remove burdens for traders, which includes the removal of all forms of authentication when it is not pertinent to the content of the exchange or the relationship between the actors, it also does recognize the need for higher levels of securisation in certain electronic exchanges. Such higher levels of securisation should be justifiable in each case and certainly not generalized to all exchanges.

To achieve this purpose, UN/CEFACT develops recommendations, white papers, green papers, guidelines and other guidance material. Together with UNECE Recommendation 14 on the Authentication of Trade Documents, the current white paper is proposed to satisfy the needs of businesses and governments when higher levels of reliability are required.

This paper is intended to help facilitate and encourage constituting a transboundary trusted environment for the international *legally significant*[2] exchange of electronic documents and data between public authorities, natural and/or legal persons. This paper may attract attention of an audience that is involved/interested in the establishment and operation as well as in the practical usage of such transboundary infrastructures.

~~To be written by the UNECE Secretariat.~~

~~[1] *Words in italics* are defined for the purposes of this paper in annex.Italic face tags the terms defined in the current Recommendation~~

[2] *Words in italics* are defined for the purposes of this paper in annex.

Table des matières

I. Introduction

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 there ~~is~~ are a number of organizational and legal issues preventing their wide usage in those activity areas where users need a certain *degree of confidence* in each other and in 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 one – by interaction of participants acting under jurisdictions of different states.

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

- Electronic tendering procedures, especially the cases when the contracting authority is a governmental body or a big company. These contracting authorities ~~lay~~ usually lay down a higher level of requirements for economic operators' trade documents validity verification.
- Certain t~~T~~rade and transport documents exchanged within cross-border trade procedures.
- Dispute resolution and settlement procedures including on-line dispute resolution. These procedures require a univocal identification and authentication of a plaintiff and defendant.
- Electronic insurance. There should be a mechanism for a reliable verification of an insurance certificate.

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 ESCAP. One of the purposes of this ~~Recommendation~~ white paper is to support governments, regional and international organizations in building up and managing these environments in an interoperable way.

UN/CEFACT recognizes the aim of removing any additional rulings, contracts or practices for facilitation of international trade procedures when possible. In particular, it is stated in ~~the~~ Recommendation 14. Nevertheless, there are still sufficient trade related scenarios whose participants seek ~~for~~ a high *degree of confidence* in each other. The current white paper ~~Recommendation~~ facilitates the implementation of exactly such scenarios.

~~Part one: Recommendation № ____ : Recommendation for ensuring legally significant trusted trans-boundary electronic interaction~~

~~I. Scope~~

This ~~Recommendation~~ white paper explores ~~seeks to encourage the use of electronic data transfer in international trade scenarios which require a high *degree of confidence* in counterparts by recommending to Governments~~ the principles of establishing and operating regional and global coordination organizations for ensuring trust in international exchange of data and electronic documents between participants (entirety of public authorities, natural and legal persons interacting within relations arising from electronic interaction).

This ~~Recommendation~~ white paper covers mainly organizational and partially technical provisions concerning trusted information and communication technologies (hereafter ICT) services. Provisions regarding establishing appropriate legal regimes may be elaborated by other~~specialized UN bodies (such as UNCITRAL)~~.

The general purpose of this ~~Recommendation~~ white paper is to help ensure the rights and legal interests of citizens and organizations ~~under the jurisdiction of United Nations Member States~~ while

performing *legally significant*[3] information transactions in electronic form using the Internet and other open ICT systems of mass usage ~~and operating within the context of a *Common Trust Infrastructure*~~.

~~II. Benefits~~

~~Harmonized regional and global coordination based on common principles will provide a smooth, transparent and reliable environment for electronic activities in transboundary trade scenarios. This will help to facilitate attaching *legal significance* to an electronic interaction between legal entities and other economic operators regardless of their location and jurisdiction.~~[4]

~~III. Use of International Standards~~

~~The use of international standards can play a key role in larger acceptance of chosen solutions and eventually interoperability. Insofar as possible, all actors, who intend to use electronic data transfer in international trade scenarios, should try to make use of existing international standards.~~

~~IV. Recommendation~~

In order to achieve ~~UN/CEFACT recommends to governments and entities engaged in the international trade and movement of goods, providing services and payment processing and seeking~~ a higher *degree of confidence* in electronic interaction, this white paper explores establishing a *Common Trust Infrastructure* (hereinafter *CTI*) - a fundamental, easily scalable platform that includes dedicated trusted ICT services and provides a unified access to these services.

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

- ~~CTI establishment principles;~~
- ~~CTI coordination approaches;~~
- ~~approaches ensuring technical interoperability of CTI services;~~
- ~~*levels of trust* provided by CTI;~~
- ~~standardization organizations to co-operate with.~~

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

~~Part 2: Guidelines on how to implement the Recommendation~~

II. Basic principle of Common Trust Infrastructure~~Introduction~~

Participants in electronic interactions typically deal with some kind of ICT services (email, cloud storages, web-portals etc.). If such participants already have a sufficient *degree of confidence* in each other and in ICT services they use, then nothing ~~is~~ 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 on the whole. The services provided by these trusted third parties are called *trust services*.

---

[3] Note that attaching the attribute "legal significance" to an electronic interaction will require a legal framework that is separate from and in addition to this white paper.

~~[4] Note that attaching the attribute "legal significance" to an electronic interaction will require a legal framework that is separate from and in addition to this Recommendation.~~

~~Under this Recommendation~~Within this white paper, *trust services* may be of different types (i.e. 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 down 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*.

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 infrastructural platform providing a unified access to *trust services*.

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

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

This institutional guarantee is proposed to be ensured within 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 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~~ any fact of electronic interaction within the *CTI* should be recorded and available for conflict resolutions if necessary.
- **Cost efficiency**. While making decision on a concrete variant of ~~the~~ *CTI* architecture, ~~variants (varies?) comparison of~~ the risk analysis should be taken into account. The *CTI* forming and functioning costs should be lower than possible losses caused by ICT-specified malfunctions and malicious activities.
- **Complexity**. Coherent elaboration of legal, organizational and technological issues should be done within *CTI* establishment. A complex description allows correct functioning of the system as a whole and its single elements.

IV~~II~~. *Common Trust Infrastructures* coordination approaches

The *CTI* architecture is selected according to the ~~principals~~ principles stated in the previous section~~Part two, chap. II above~~. There are three levels of *CTI* coordination: legal, organizational and technological.

Legal level

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.

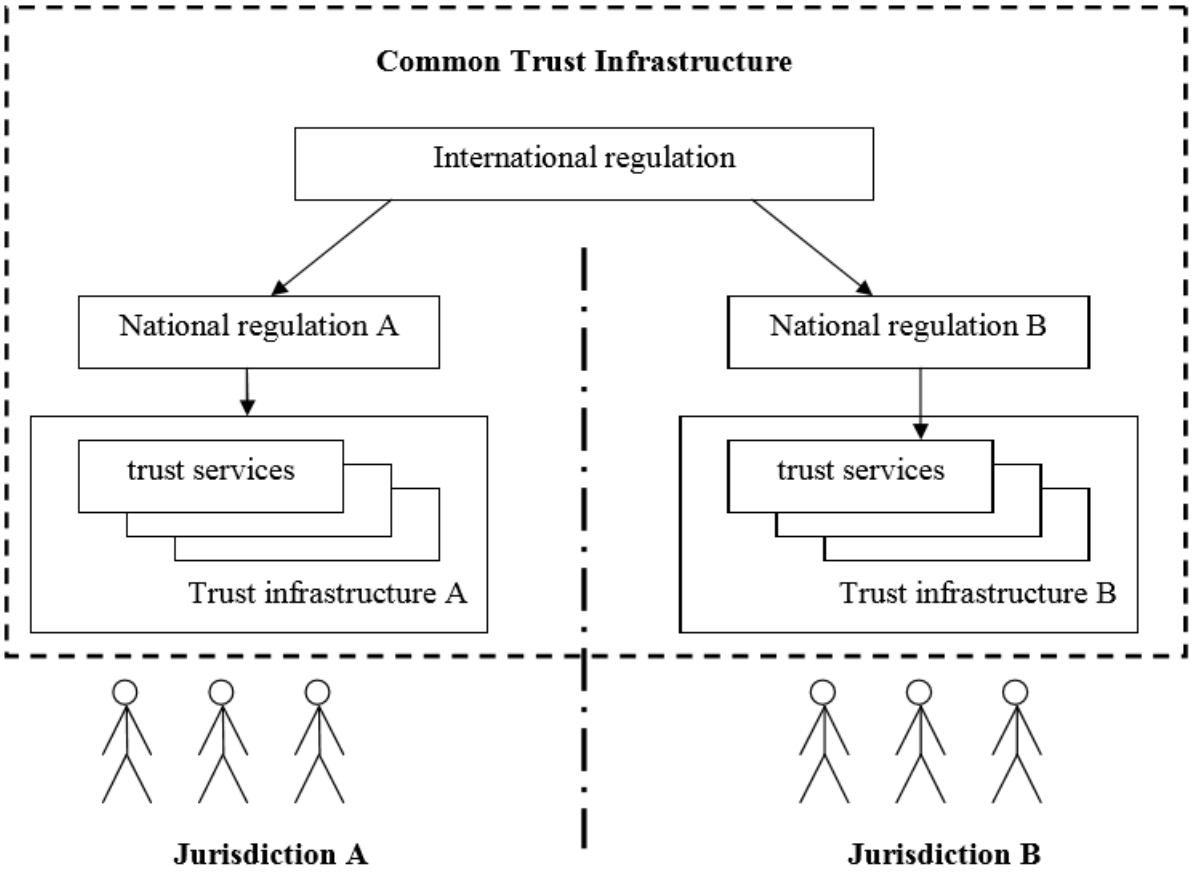

FIG.1. LEGAL LEVEL

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.

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

~~We recommend a tight cooperation with UN bodies specialized in legal frameworks elaboration (such as UNCITRAL) in order to harmonize the effort of this Recommendation concerning the necessary coordination on the legal level, see Part two, chap. VI.~~

Organizational level

Mutual *legally significant* recognition of electronic documents and data treated by *trust services* provided under various jurisdictions could be ~~is~~ reached through creation and operation of a dedicated body (let's call it ~~International~~ a CTI Coordination Council or CTI-CC) that includes national regulation bodies having voluntarily joined~~ted~~ the CTI-CC. The activity of CTI-CC could be~~is~~ regulated by ~~the~~ a CTI-CC Statute which ~~could~~ should ~~is to~~ 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.

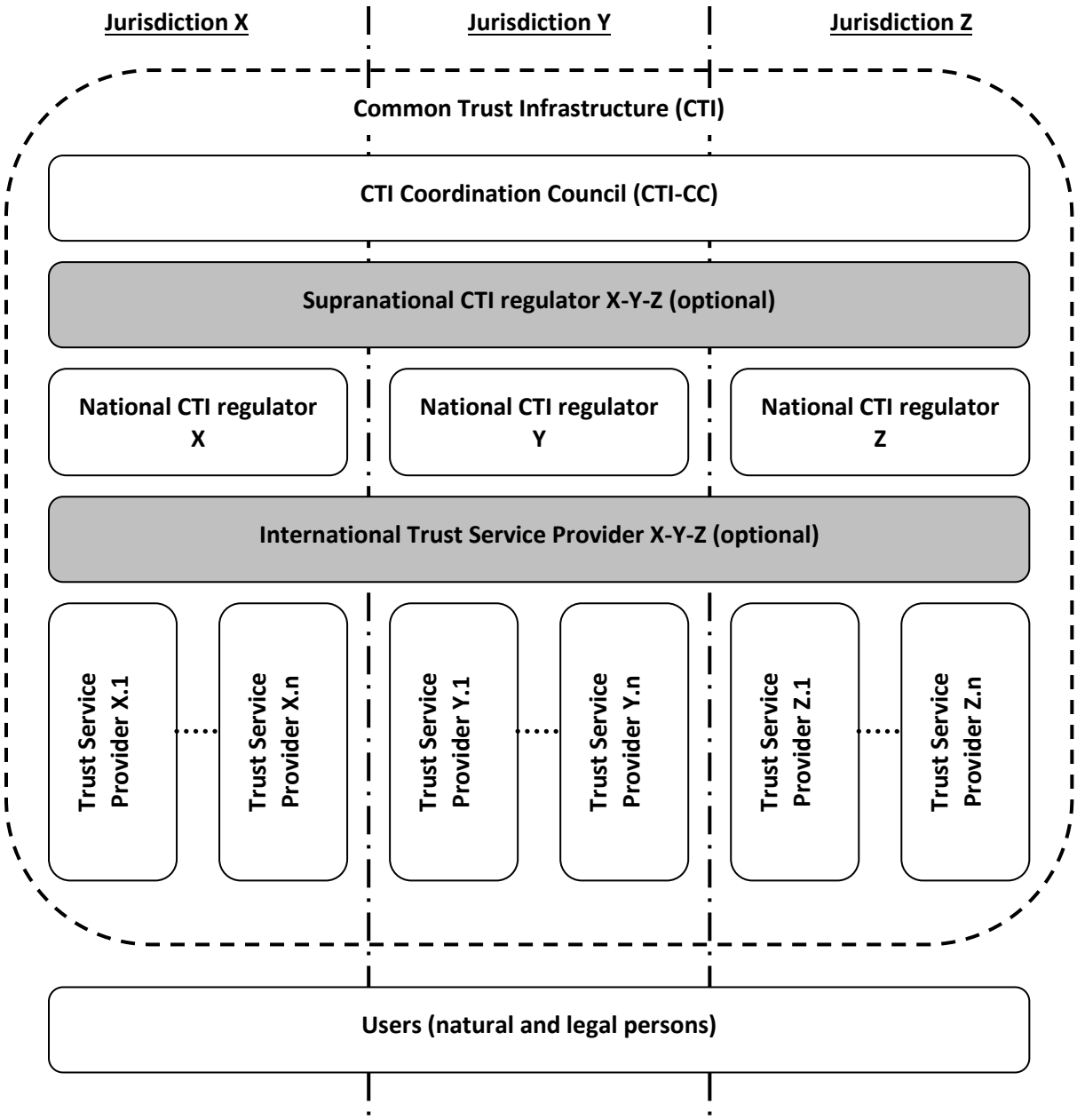

Fig.2. Organizational level (optional elements are identified by the grey blocks)

The ~~ICC~~CTI-CC issues a number of documents interconnected with its Statute:

- **Requirements** for the ~~ICC~~CTI-CC members, correspondence to which is a prerequisite for the full membership in the ~~ICC~~CTI-CC;
- **Guidelines** on carrying out 'shadow' supervision for admittance to the ~~ICC~~CTI-CC and periodic mutual audit for maintaining voluntary membership in the ~~ICC~~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.

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

For groups of states with high degree of integration (for example, Eurasian Economic Union member-states or European Union member-states) there is the possibility of constituting a Supranational *CTI*

regulator (see. Fig. 2, Supranational *CTI* regulator X-Y-Z). In such case, one Supranational *CTI* regulator X-Y-Z substitutes a group of National *CTI* regulators X, Y and Z.

The natural *CTI* scalability is enabled through the procedure for admitting new members to the ~~ICC~~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 ~~ICC~~CTI-CC (new providers of the *trust services*).

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

Inter-domain gateways can be established both: at only legal and organizational levels and at a complex level: legal, organizational and technical one.

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

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

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. of an environment outside (beyond) any single *domain*. The ~~ICC~~CTI-CC and International trust service providers represent parts of this neutral international environment. Such a neutral international environment could~~shall~~ be operated in a neutral legal field that is defined by an international body~~, for example, by a UN Convention or by an international treaty between single countries or unions of countries, see sec. 'Legal level' above~~.

I.e. in the case, when 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 to be a gateway.

In the second 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 fulfill the requirements (attributes, format, structure, etc.) for *legally significant* electronic documents in recipient's *domain*[5] (jurisdiction). In such a way the inter-domain gateway *trust service* can substitute a number of *trust services* that provide only single specific functions (e-signature verification, powers verification, time stamping etc.). As ever, even technically implemented inter-domain gateway *trust service* shall also be operated in a neutral international environment.

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

In order to become a National Trust Service Provider, a supplier of the respective services ~~shall~~ should undergo accreditation with the National *CTI* regulator of the same jurisdiction. International

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

Trust Service Providers ~~shall~~ should undergo accreditation with the ~~ICC~~CTI-CC. The requirements for accreditation of the providers of the *trust services*, as well as the requirements to their activity ~~are~~ should be regulated by the *Compliance criteria* issued by the ~~ICC~~CTI-CC and possible national supplements issued by the respective National *CTI* regulator.

In the ~~ICC~~CTI-CC, the users of electronic services ~~can~~ could ~~be~~ 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.

The services ~~are could~~should be provided by the respective suppliers – the *trust service* providers. The *trust service* providers ~~are could~~should be integrated by the *CTI*.

The *trust services* as the *CTI* elements ~~can~~ could have different variants of realization depending on the *level of trust* between *domains* (jurisdictions). For example, with conditionally 'high' or 'medium' level of mutual trust between the *CTI* members, it is efficient to use centralized International *trust services* applied according to the standards agreed upon. In case of conditionally 'low' *level of trust*, the *trust services* are built according to the decentralized principle – national *trust services* in each single jurisdiction.

Technological level

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

~~We~~ This white paper recommends a tight cooperation with major organizations in the area of technical standardization such as ISO, ETSI, W3C, CEN and others in order to harmonize the effort of this ~~R~~recommendationpaper concerning the necessary coordination on the technological level~~, see Part two, chap. VI~~.

~~I~~V. Trust infrastructures services technical interoperability ensuring approaches

To work out *trust services* types it is proposed to consider base document's attributes that are usually necessary to provide document's legal function fulfillment.

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, which is to be irrespective ~~to~~ of an expression form – whether paper or electronic one: 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 point 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 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.

Table 1: document’s attributes needed for providing document’s legal function fulfillment

Document’s attributes above can be verified by *trust services* of different types.

Basic *trust services* types (trust services functions provided dependent 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.
   If there is a gateway between *domains* (jurisdictions), there should be a profile for this inter-domain gateway based on 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 ~~shall~~ ~~could~~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 ~~1~~2. *Trust services* (incl. 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 ~~or~~ and legal persons.

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.

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 ~~ICC~~CTI-CC shall decide/agree on eligible identification schemes including minimal requirements on them. There may be ~~ICC~~CTI-CC own identification schemes and/or references to international standards and/or references to the notified identification schemes inside the single *domain*.

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 directed, besides others, on personal data protection.

Note. Long time archival and related verification service can be realized as a function of ICT service or as a function of a special trust service type.

Note. The existing electronic systems should be taken into account; so the requirements on their updating for connecting to the *CTI* may be minimal.

VI. Common Trust ~~i~~Infrastructure~~s~~ services levels of qualification

The *level of qualification* of a *trust service* is a property of the trust service to evidently fulfill a pre-defined set of requirements on it.

There may be different incremental *qualification levels* of a *trust service*. The lower is the degree of confidence of the participants in each other and in the ICT services processing electronic interaction (creation, access, transformation, transmission, destruction, etc.), the higher might be demand~~ed~~ on the *qualification level* of *trust services*.

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

	Degree of confidence of participants 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~~.~~[6]
Organizational architecture of trust	n.a.	Large Scale Projects of any kind	CTI-~~International~~ Coordination Council (~~ICC~~CTI-CC), see ~~Part two, chap.~~ Title ~~II~~IV above

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

services			
Technological requirements on trust services	n.a.	Meet the recognized best practices for trust service providers~~.~~	-- Meet ~~ICC~~CTI-CC Compliance Criteria AND -- Meet the requirements laid down in the applicable national regulation (for national trust service providers)~~.~~

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

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

~~Communication with UN bodies specialized on legal frameworks elaboration~~

1) ~~It is recommended~~This white paper suggests ~~to give~~ giving 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.

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

Established legal regimes can also provide for imposing special requirements on the material and financial support of the business activity of specialized providers in case of damage to their users, including cases of compromising personal data.

Issues of institutional guarantees and legal regimes for constituting and functioning regional and global transboundary trusted environment are proposed to be considered in a separate document by a specialized ~~UN~~ body.

2) ~~It is recommended~~This paper suggests ~~to describe~~ describing the mechanisms of interaction of particular states and their international unions with other international formats in the frames of constituting ~~of~~ a common transboundary trusted environment:

2.1) 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 ~~which~~ frames 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.

2.2) On the basis of interaction between different international unions:

- in the first stage, a group of states creates a~~n~~ 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 regard to institutional guarantees and information security requirements appertaining

to each of the international formats, possibly on the basis of an inter-domain gateway being operated in the frames of an international legal regime.

2.3) On the basis of interaction of a state with other states or international unions:

- in the first stage, a state creates its own *domain* functioning in the frames of 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 ~~-~~regard of ~~to~~ institutional guarantees and information security requirements appertaining to these states and international formats, possibly on the basis of an inter-domain gateway being operated in the frames of an international legal regime.

3~~) It is recommended~~This paper suggests ~~to describe~~ describing *domain*-constituting mechanisms, similar to item 2), for legal regimes based on commercial agreements and/or common trade practice.

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

~~It is recommended~~This white paper suggests ~~to take~~ taking into consideration the following aspects of standardization:

1. Technical and technological aspect

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.

2. Organizational aspect

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

The specified aspects should be considered as 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 tags the terms defined for the purposes of this white paper~~in the current Recommendation~~.

For the purposes of this ~~document~~ 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 technical / technological levels to its users.

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 unit) 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)

- ~~*Legal validity* (also called 'legal force') is~~ 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 fulfill a pre-defined set of requirements on it. 438

~~-~~***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 is 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 ~~purposing proposing~~aiming to ensure a certain *degree of confidence* between the participants of electronic interaction.

trusted electronic interaction

- the exchange of any data in electronic form in such a way that a user of these data undoubtedly accepts them according to its operational policy. Each user's operational policy determines whether the electronic interaction is considered as 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 technologies services (such as an internet provider, email provider, message exchange services of any kind, cloud storages, etc.). But *trusted electronic interaction* is provided by using *trust services*.

ANNEX ~~1~~2 -

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 – the set of requirements for domain B and E(a) is the set of transformation rules from A to B. Taking in mind that powers of sets (i.e. quantity of requirements in a real word) can be not equal (N <> M), there should be rules defined to lead both sets to equal power K where K:=MAX(N, M).

- The degree of trust to such 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 universal superset of requirements for A and B.