Recommendation for ensuring legally significant trusted trans-boundary electronic interaction

draft
version 0.94

Lance comments in general:
This document reads much more like a technical implementation guideline than a recommendation.

- UN/CEFACT recommendations' guidelines do not start out with a list of definitions (that is typical of ISO recommendations)
- The technologies which could respond to the principles outlined in this document do not seem to be technology neutral (pre-requisite for all recommendations). The entire list of authentication typologies in Annex B.2 of Rec14 would not be able to apply to this document.
- Table one of this document which lists the minimum attributes clearly reflects that the resulting authentication method is not technology neutral. Only certain technologies can respond positively to this list.

There is no clearly defined recommended practice besides that every nation should establish a CTI – this is in direct contradiction with Recommendation 14, paragraph 9 and many other UNECE recommendations which push to eliminate authentication as much as possible.

Other UNECE Recommendations do not seem to be referenced. There is not one reference to Rec14 – and this document is clearly addressing authentication of trade transactions. So what is the relationship with Rec14? I am missing how this document will enhance the guidance provided in Rec14.

This subject matter is also very closely related to several works of UNCITRAL. Where are the references to these documents and model laws? How does this document enhance the work done within UNCITRAL? (and as a side note, we cannot recommend to UNCITRAL to start new work items – we only reference their deliverables or their current work items)

Proposed way forward:

- As it is written at this time, I do not see this as a recommendation. Either a lot of work will have to be undertaken, or the project team may want to consider revising their project proposal in order to create a "Technical Implementation Guide" instead of a recommendation.

Contents

Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3
Удалено: 3

Foreword

This Recommendation is intended to help facilitate and encourage constituting a transboundary trust space for the international legally significant exchange of electronic documents and data between public authorities(why only public authorities?), physical 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 general purpose of this Recommendation 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 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 (How this can be achieved at global level ?).

This institutional guarantees are proposed to be ensured within business activity of specialized operators(How specialised operators can be regulated; difficult to achieve) 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.

This Recommendation covers only the organizational and partially technical[1] provisions concerning trusted ICT services. Provisions regarding establishing appropriate legal regimes may be subject matter of a separate dedicated Recommendation by UNCITRAL(How can you force UNCITRAL to do this. You can only operate under current UNCITRAL framework).

Participants in electronic interactions typically deal with some kind of ICT services (email, cloud storages, web-portals etc.). If such participants have a high degree of confidence in each other and in ICT services they use, then nothing is 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 third party to help increase the degree of confidence in the electronic interaction on the whole. The services provided by these third parties are called trust services(difficult to create institutional arrangements for getting service levels).

Under this Recommendation, trust services may be of different types (provide different functions) and of different levels of qualification. High level qualification trust services operate under one or more international legal agreements, and they meet the requirements and follow the rules laid down by some international coordinator(you are proposing to create an international trusted regulator, which is difficult to achieve). Basic level qualification trust services operate under one or more commercial agreements(how to achieve this ?), and they can be established within some large scale international projects(who will pilot and sustain this ?) and follow the recognized best practices for trust service providers. Trust services should be audited in accordance with their level of qualification(how to achieve?).

The aggregate of trust services operating within the legal, organizational and technical framework forms the Common Trust Infrastructure (hereinafter CTI)(Who regulates this and

[1] UN/CEFACT covers technical provisions in semantic interoperability layer only.

Примечание [LT1]: The Summary is usually written by the UNECE Secretariat based on the content of the document. It is often much shorter…

Примечание [LT2]: This sounds as if the UN would be directly involved in such assurance. Should be under the jurisdiction of a given state…

Примечание [LT3]: All abbreviations must be defined at least at first usage.

Примечание [LT4]: It seems strange to have a footnote in a foreward. And the footnote is using a term which others might not understand (semantic layer)…

Примечание [LT5]: Unless UNCITRAL has announced that they are working on this, it is not the place of UN/CEFACT to suggest topics for their consideration…
Completely agree with TAKhan comments.

Примечание [LT6]: This text is to become part of a large group of recommendations, in which Rec14 clearly defines this situation. The term chosen within Rec14 was “levels of reliability” as this term does not have any other technical signification. See Rec14, page8
It would be advisable to use the same terms as defined in previous recommendations.

Примечание [LT7]: This is a technical term. Non-technical readers of this recommendation may misunderstand what this means. The target audiences for recommendations are high-level deciders (and not technical practitioners).

Also, is this really generic? Would all third parties offer “trust services”? Are there not other services which might be provided?

Примечание [LT8]: What may be considered a high level in one country may not be the same in another country. I do not believe that this assertion is correct in today’s environment. Unless the text is going to propose how to achieve this – which would likely be more a legal matter.

who updates this with technological advancements). The CTI is a fundamental, easily scalable infrastructural platform providing a unified access to trust services.

1. Recommendation № ___ : Recommendation for ensuring legally significant trusted trans-boundary electronic interaction

1.1. Scope

This Recommendation seeks to encourage the use of electronic data transfer in international trade scenarios by recommending to Governments the principles of establishing and operating regional and global coordination organizations(who will fund and run this regional and global coordination organisationand how to ensure trust among parties ?) for ensuring trust in international exchange of data and electronic documents between participants. This Recommendation covers only the organizational and partially technical provisions concerning trusted ICT services. ≤Provisions regarding establishing appropriate legal regimes may be the subject matter of a separate dedicated Recommendation by UNCITRAL(Are we expecting too much from UNCITRAL ?).

1.2. Benefits

Harmonized regional and global coordination based on common principles will provide a smooth, transparent and reliable environment for electronic activities in trans-boundary 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[2].

1.3. 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, legal entities and other private actors(Initial expectations indicated are for Public authorities only ?) who intend to use electronic data transfer in international trade scenarios should try to make use of existing international standards (which standards and who prescribed from time to time).

1.4. Recommendation

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*.

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

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.*

The CTI is a fundamental, easily scalable platform providing a unified access to trust services. Herewith, the existing electronic systems are taken into account, so the requirements to their updating for connecting to the CTI are expected to be minimal(Who regulates or facilitates and ensures compatibilities ?).

[2] 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 (it is difficult to achieve ?).

Примечание [LT9]: The section SCOPE should provide the basis of what this recommendation is seeking to achieve. The paragraph here is very general and does not give much indication on how such trusted transactions are to be achieved.

Примечание [LT10]: This is a very strong statement.
In the past, UN/CEFACT has always encouraged companies to remove administrative burdens to traders, not create new ones.
UN/CEFACT has also encouraged removing the need for authentication altogether on documents related to international trade. This is clearly outlines in Rec14, page 12 as well as in other UNECE Recommendations.

Примечание [LT11]: Authent ication is only one method of ensuring trust. There are others.

Примечание [LT12]: Unless this work already exists or has been announced at UNCITRAL, which I do not think is the case, this phrase cannot be written.

Примечание [LT13]: This section should point to places where the trader can find the relevant international standards. Do these exist already? Where should the operator look to find them? ISO? Others?

Примечание [LT14]: I do not see a formal recommended practice besides the establishment of CTI… and this is not possible as it would contradict Rec14 paragraph 9.

Примечание [LT15]: Such a phrase will result in some of these ‘regions’ requesting examples of how the regional peculiarities result in different levels of trust. It might be advisable to avoid such sweeping statements unless there are concrete examples to back them up.

Примечание [LT16]: NO. UN/CEFACT would not make such a recommendation.
UN/CEFACT would recommend to eliminate as much as possible the need for authentication – this is clearly the first recommendation of Rec14 (paragraph 9).
Establishing and using CTI cannot be, as is, a recommendation of UN/CEFACT as this would contradict Rec14, paragraph 9.
... [1]

Примечание [LT17]: This sounds very technical. The recommended practice should be plain text which any implanter would be able to understand. Not sure this is the case here.

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

– CTI establishment principles;

– CTI coordination approaches;

– approaches ensuring technical interoperability of CTI services(How to achieve ?);

– levels of trust provided by CTI;

– standardization organizations to co-operate with(How ?).

2. Guidelines on how to implement the recommendation

2.1. Terms and Definitions[3]

For the purposes of this document 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(How to maintain and update and derive trust ?).

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.

electronic interaction

– the exchange of electronic information between two or more parties facilitated by the use of information and communication technologies (ICT). ICT refers to technologies that provide information processing (creation, storage, access, transformation, transmission, destruction, etc.) in the telecommunication context[4]. Any electronic interaction utilizes *ICT services* (such as an internet provider, email provider, message exchange services of any kind, cloud storages, etc.).

legal significance (of an action)

– a property of an action (of a process) to originate (to result in) documents (*data unit*) possessing *legal validity* *(how to define and ensure acceptability ?)*.

legal validity (of a document, or, generally, of data)

– 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) (how to enforce between bilateral or multilateral context ?).

level of qualification (of a service)

Примечание [LT18]: NON. This cannot be the recommended practice. UN/CEFACT already recommends to remove the need for authentication when possible. So we cannot simultaneously encourage putting in place a CTI.

Примечание [LT19]: This is reading like an ISO recommendation. To my knowledge, UN/CEFACT does not normally start off its Guidelines with a list of terms and definitions.

Such a list is not acceptable in a UN/CEFACT Recommendation. The definitions should be presented within their context as is the case in other UNECE recommendations.

Примечание [LT20]: What are these 'trust services?'

Примечание [LT21]: The concept described below is already defined as "levels of reliability' in Rec14 (see p.8).
Why is a new term being created instead of pointing to what we already have in our recommendations?

Примечание [LT22]: Why a societal function?

Примечание [LT23]: Why are we not referring to UNCITRAL work when we are discussing legal significance or legal validity? I believe that legal validity is at least touched on in the Model Law on authentication. Is it not?

Примечание [LT24]: The term and the definition are confusing. An example would be helpful.

[3] *Italic face* tags the terms defined in the current Recommendation
[4] 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

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

levels of trust (between the *trust domains*)

– a societal function determining the degree of trust between the *trust domains*. Depending on an established level of trust, *trust domains* are prepared to share a certain amount of resources and to jointly use certain infrastructures, i.e. *trust 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 *trust domains* are prepared to delegate to the CTI(How to achieve ?).

participants of electronic interaction

– entirety of public authorities, individuals and legal persons interacting within relations arising from *electronic interaction*.

transboundary trust space (TTS)

– an aggregate of legal, organizational and technical conditions recommended by relevant specialized UN agencies (departments)(Who & how ?) and international organizations with the aim of ensuring trust (a certain degree of confidence) in international exchange of electronic documents and data between participants of *electronic interaction*.

trust service

– (high level definition) - an electronic service purposing 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(who defines and ensures compatibility ?). Each user's operational policy determines whether the electronic interaction is considered as a *trusted* one(who ensures interoperability ?). Hence, the determination of the trustworthiness of data received in an electronic exchange varies from one user to another. Trusted electronic interaction is provided by using *trust services(Who ensures this, monitors this and ensures compliances ?)*.

2.2. Common Trust Infrastructure establishment principles(How to ensure ?)

– **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 operators of trust services, and register systems.

– **Traceability**. Any fact of electronic interaction within the CTI should be recorded and available for conflict resolutions if necessary.

– **Cost efficiency**. While the CTI architecture variants comparison 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.

Примечание [LT25]: This term already has a specific meaning in ISO. Is this the same definition as within ISO? I believe that the ISO definition already has a strong technical meaning.

In Rec14, we preferred to use the term 'Levels of reliability' as this term did not yet exist.

Примечание [LT26]: Is this definition really necessary? It's not self evident?

Примечание [LT27]: The only term which does not seem to be in this list of definitions is "TRUST" and this is part of the name of the document…

Here is where we perceive how 'trust' is being defined in this document. However, I believe that the definition is much more complex. Unless, I'm mistaken, UNCITRAL was never able to agree on a definition. I do not believe that we can leave this interpretation like this.
This will cause a problem for the entire document as the word 'trust' is an integral part of the title. How to define it when UNCITRAL has not been able to…?

Примечание [LT28]: The definition is not sufficiently clear. What exactly is a trust service?

Примечание [LT29]: Should be level of reliability.

Примечание [LT30]: This phrase is false.
Trust can be established on many levels and may be because two business partners work together for many years. Their direct electronic interactions without any intermediary would also be considered a trusted electronic interaction – but there is no trust service between them..

2.3. Common Trust Infrastructures coordination approaches

The CTI architecture is selected according to the principals stated in sec. 2.2 above. There are three levels of CTI coordination: legal, organizational and technological.

Отформатировано: английский (США)

Удалено: 2.2

Примечание [LT31]: This document might want to align these levels to what is defined in Recommendation40 and which was reused in Recommendation 4. It may even allow the document to free itself from these legal issues.

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.

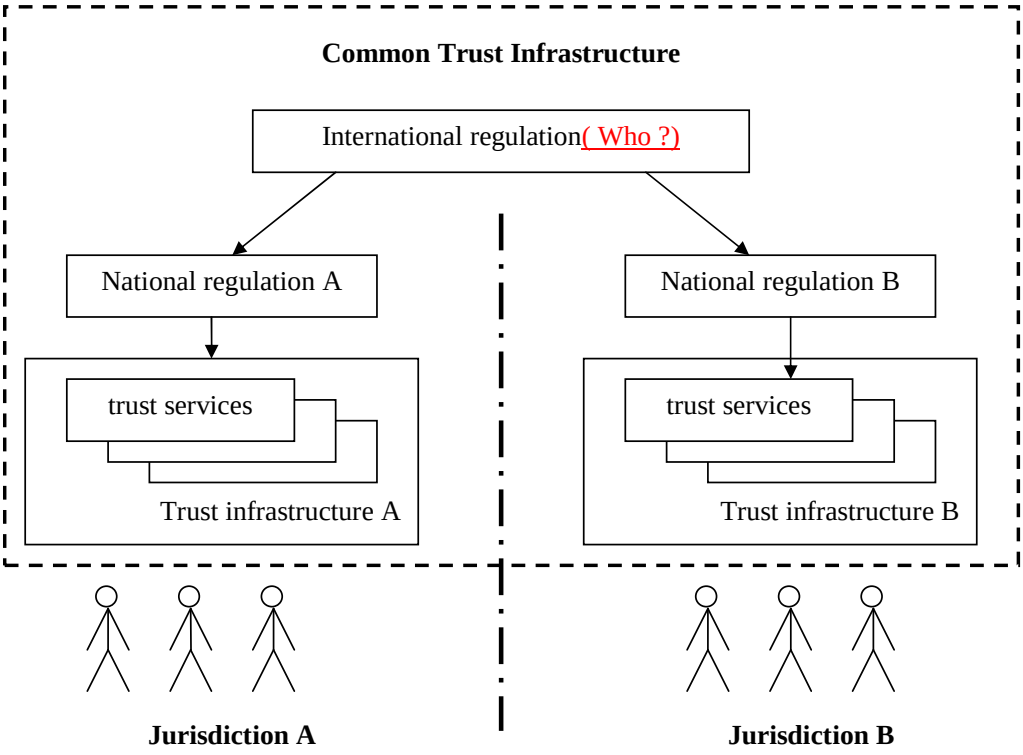


Fig.1. Legal level

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.

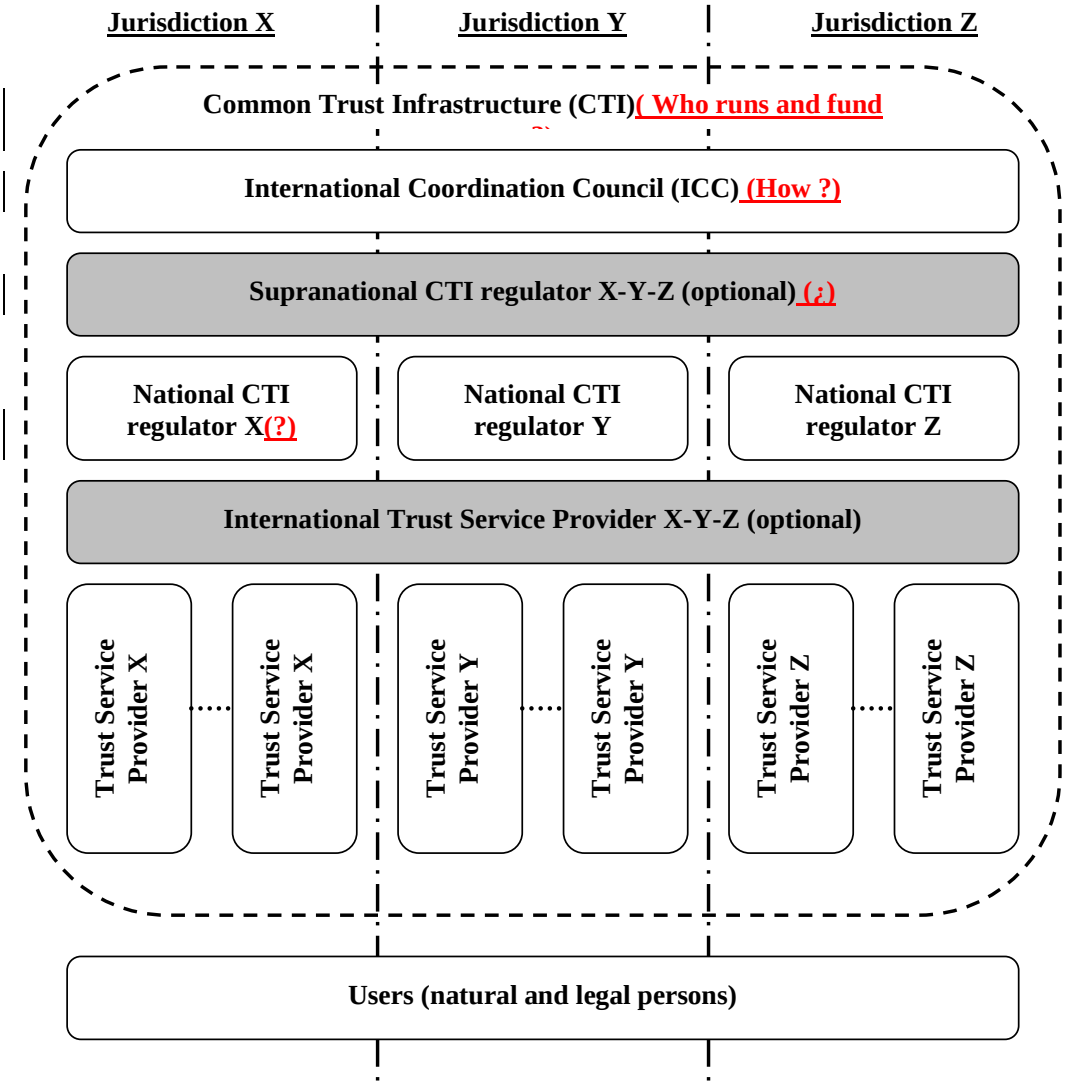
The national legal regulation is built on a complex of normative documents that are standard in each particular jurisdiction.

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

Organizational level

Mutual legally significant recognition of electronic documents and data treated by trust services provided under various jurisdictions is reached through creation and operation of a dedicated body (let call it International Coordination Council or ICC) that includes national regulation bodies having voluntarily jointed the ICC. The activity of ICC is regulated by the ICC Statute which 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(Difficult to achieve).



Примечание [LT32]: This cannot be written like this unless UNCITRAL already has a deliverable addressing this or has a work item on the table going in this direction.

Удалено: 2.6

Отформатировано: Шрифт: английский (США)

Примечание [LT33]: So one of the recommended practices is to create this supranational body? Under whose authority? The UN? The WTO? The WCO? The ITU?...? Would it be its own body? I am not sure that this is common practice in UN recommendations to make such propositions.

Примечание [LT34]: This is a bad acronym because ICC will usually mean 'International Chamber of Commerce.' This acronym should be changed in this text in order to be correctly understood.

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

The ICC issues a number of documents interconnected with its Statute:

- *Requirements* for the ICC members, correspondence to which is a prerequisite for the full membership in the ICC;
- *Guidelines* on carrying out 'shadow' supervision for admittance to the ICC and periodic mutual audit for maintaining voluntary membership in the ICC;
- *Compliance criteria* which are to be met by operators of the trust services, and the methodology for applying these criteria;
- *Scheme of estimation/verification* of operators 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 operators 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 (new national and supranational participants) and the scheme for verifying that the operators of the trust services meet the *Compliance criteria* issued by the ICC (new operators of the trust services).

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

nIDGs 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 of the TTS 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(Is this achievable ?), i.e. of an environment outside (beyond) any single domain. The ICC and International operators represent parts of this neutral international environment. Such a neutral international environment shall be operated in a neutral legal field that is defined, for example, by a UN Convention(how ?) or by an

international treaty between single countries or unions of countries, see sec. ‘Legal level’ above.

I.e. in the case, when nIDGs are established at only legal and organizational levels, these nIDGs 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 nIDGs are established at legal, organizational and technical levels, nIDGs 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 nIDG 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 nIDG trust service shall also be operated in a neutral international environment.

Approaches to forming nIDGs 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 trust levels of the identification schemes used inside the interacting domains, as well.

In order to become a National Trust Service Provider (TSP; operator of the trust service), a supplier of the respective services shall undergo accreditation with the National CTI regulator of the same jurisdiction. International Trust Service Providers shall undergo accreditation with the ICC. The requirements for accreditation of the operators of the trust services, as well as the requirements to their activity are regulated by the *Compliance criteria* issued by the ICC(difficult to achieve ?) and possible national supplements issued by the respective National CTI regulator.

In the ICC, the users of electronic services can 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 provided by the respective suppliers – the trust service providers. The trust service providers are integrated by the CTI.

The trust services as the CTI elements can have different variants of realization depending on the *level of trust* between trust 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 documents(How one funds ICC).

We recommend a tight cooperation with major organizations in the area of technical standardization such as *ISO, ETSI, W3C* and others in order to harmonize the effort of this

Примечание [LT35]: This phrase is part of the reason why UN/CEFACT cannot recommend the establishment of CTI. The involvement of third party ‘trust’ service providers defacto in the operation is in direct conflict with the principles in Rec14 (where such 3rd parties are only used if desired by the traders or required by the states) and the principles in several other recommendations that seek to eliminate such burdens to transactions.

Примечание [LT36]: Where are these centralized and decentralized models described?

Примечание [LT37]: These should be mentioned in the “Use of International Standards” in the beginning of this text.

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

Recommendation concerning the necessary coordination on the technological level, see sec. 2.6.

Отформатировано: Шрифт: английский (США)

Удалено: 2.6

2.4. Trust infrastructures services technical interoperability ensuring approaches

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

№	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 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) logotype 2) name of a issuer 3) issuer reference data (address, contacts etc.) 4) seal impression It can be performed through constituting of an authorized body that provides electronic register assuring the attribute validity property. or For electronic seals it can be fixed with a special attribute in electronic seal certificate.
3.	Signatory status (powers) or signatory position	no	Can be performed through forming of an electronic register of authorized persons or roles, containing a brief description of powers with their duration stated. or Can be fixed with a special attribute in electronic signature certificate.
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) electronic seal of issuing organization 7) etc. Can be performed through using of an electronic signature (for natural persons) and/or electronic seal (for

№	Attribute type	Mandatory yes/no	Description/comments
			legal entities). Note: The form of the relationship between the signatory and the document content (negotiation, approval, visa, copy legalization, etc.) can be stated in a document body, included to an electronic signature/seal or reflected in metadata to a record in an electronic data base.
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. There would be at least a theoretical opportunity for TSPs for offering – similarly to the time stamp service - a 'place stamp service' based on a trusted geo position source (e.g. a global navigation satellite system (GNSS)). 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

Documents 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 electronic signatures and seals.

b) Monitoring of legal status.

c) Creation, verification, and validation of electronic time stamps.

d) Providing neutral inter-domain gateways (nIDG).

If there is a gateway between domains (jurisdictions), there should be a profile for this nIDG based on agreement between these domains. Each nIDG profile should "know" what attributes are mandatory for each domain. On the technological level, a nIDG shall implement some protocol translation or translation of different protocols or standards from one domain to another. For mathematical description of nIDG functions please refer to ANNEX 2. Trust services (incl. nIDGs) 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 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 operators specialized in performing identification. These services can

Примечание [LT38]: These trust services do not seem to be technology neutral to me. I would like to know how any of the authentication methods in annex B.2 of Rec14 can respond to the requirements listed in table one above.

Примечание [LT39]: I believe that this is a misuse of this term. What is truly meant here is 'digital signature' given the conditions listed above.

Удалено: Table 1

be implemented on different qualification levels: zero, basic and high. The ICC shall decide/agree on eligible identification schemes including minimal requirements on them. There may be ICC own identification schemes and/or references to international standards and/or references to the notified identification schemes inside the single trust domains.

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 trust domains. Sets of identification attributes can be defined by the legal regimes for the business activity of operators specialized in performing identification and of functional operators. Sets of identification attributes can be maintained by the trust services (identification service). The activity of operators 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.

2.5. Trust infrastructures 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 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 services	n.a.	Large Scale Projects of any kind.	International Coordination Council (ICC), see sec. 2.3 above
Technological requirements on trust services	n.a	Meet the recognized best practices for TSPs.	– Meet ICC Compliance Criteria AND – Meet the requirements laid down in the applicable national regulation (for national TSPs).

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

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

Отформатировано: Шрифт: 10 пт, английский (США)

Удалено: 2.3

Примечание [LT40]: I do not understand how to read this table. What are the headings of each column/line?

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

2.6. Communication with organizations in different areas of standardization

Communication with UNCITRAL on legal regulation

1) It is recommended to give 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 operators 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 TTS-domains are proposed to be considered in a separate UNCITRAL Recommendation.

2) It is recommended to describe the mechanisms of interaction of particular states and their international unions with other international formats in the frames of constituting of a common TTS:

2.1) By means of the complete or a partial joining a state to an existing legal regime on the basis of international treaties and/or directly applicable international regulations, in which frames a task on forming a regional TTS 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 an regional TTS 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 a nIDG 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 trust 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 regard to institutional guarantees and information

Примечание [LT41]: UNCITRAL is in the title, but I do not see any references to UNCITRAL work in the text.

Примечание [LT42]: Please cite the completed recommendation name and date.

security requirements appertaining to these states and international formats, possibly on the basis of a nIDG being operated in the frames of an international legal regime.

3) It is recommended to describe 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 trust space

It is recommended to take 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 trust space. 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 trust domains being sufficient for a mutual recognition (legalisation) of electronic documents and data, which are issued in different domains or 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 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 1

Mathematical description of nIDG functions

Примечание [LT43]: One needs what level of mathematical skills to understand these formulas?

- The set of rules to translate the related requirements between two domains A and B should be laid down within nIDG

  $A:=\{a_1, a_2,..., a_N\}$
  $B:=\{b_1, b_2,..., b_M\}$
  $E(a):=A \rightarrow B$
  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.

Стр. 5: [1] Примечание [LT16] **Lance Thompson** **18.11.2015 15:20:00**

NO. UN/CEFACT would not make such a recommendation.
UN/CEFACT would recommend to eliminate as much as possible the need for authentication – this is clearly the first recommendation of Rec14 (paragraph 9).
Establishing and using CTI cannot be, as is, a recommendation of UN/CEFACT as this would contradict Rec14, paragraph 9.

It would be possible to say here that not all transaction require authentication, but where it is justified by the context of the transaction, one method or establishing such authentication could be through CTI.