Recommendation for ensuring legally significant trusted trans-boundary electronic interaction

draft

version 0.9

Contents

Foreword

Executive summary

The general purpose upheld by this Recommendation is to guarantee ensuring 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.

This institutional guarantees are proposed to be ensured within business activity of specialized operators 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.

Current Recommendation covers only the provisions concerning trusted ICT services. Provisions regarding establishing appropriate legal regimes may be subject matter of a dedicated Recommendation by UNCITRAL.

Any participants of electronic interaction deal with some kind of ICT services (email, cloud storages, web-portals etc.). If participants have a high degree of confidence in each other and in ICT services they use, then nothing is to be changed. But if participants are not sufficiently confident in each other and/or in ICT services, then there should be a third party increasing the degree of confidence in electronic interaction on the whole. The role of these third parties play trust services.

Trust services may be of different types (provide different functions) and of different levels of qualification. High level qualification trust services operates under some international legal agreements, they meet the requirements and follow the rules laid down by some international coordinator. Basic level qualification trust services operates under some commercial agreements, they can be established within 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 with the legal, organizational and technical framework operates forms the Common Trust Infrastructure (hereinafter CTI). 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 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.

1.2. Benefits

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

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 and private actors who intend to use electronic data transfer in international trade scenarios should try to make use of existing international standards. Technical standards which were able to be identified during the development of this Recommendation are referenced in Annex B.

1.4. Recommendation

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

To Governments and entities engaged in the international trade and movement of goods, providing services and payment processing and willing a 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).

The primary objective of CTI is ensuring *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.

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.

2. Guidelines on how to implement the recommendation

2.1. Terms and Definitions[1]

For the purposes of this document the following terms apply:

Common Trust Infrastructure (CTI)

- infrastructure ensuring 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.

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

degree of confidence (of the participants of *information interaction* in each other and in the ICT services processing *electronic interaction* between them)

- a societal function of an established or felt degree of confidence of the participants of *information interaction* in each other and in the ICT services processing *electronic interaction* between them.

electronic interaction

- a way of *information interaction* based on use of information and communication technologies (ICT). ICT refers to technologies that provide information processing (creation, access, transformation, transmission, destruction, etc.) in the telecommunication context[2]. Any electronic interaction deals with *ICT services* (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*.

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).

level of qualification (of a service)

- 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 domain*. 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.

transboundary trust space (TTS)

- an aggregate of legal, organizational and technical conditions, harmonized by the member-states in order to ensure trust in international exchange of data and electronic documents between authorized bodies.

[2] 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

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. It is a matter of a concrete Operational Policy, which way is considered as a *trusted* one. Hence, the determination of the trustworthy of some data varies from one concrete case to another. Trusted electronic interaction is provided by using *trust services*.

2.2. Common Trust Infrastructure establishment principles

- **Scalability**. The CTI is 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 data exchange within the CTI should be fixed and available for conflict resolutions if necessary.
- **Cost efficiency**. While the CTI architecture variants comparison the risk analysis should be taken into account.
- **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.

2.3. Common Trust Infrastructures coordination approaches

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

Примечание [s1]: *=global*

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

Примечание [s2]: From the project proposal

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.

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 legal regulation.

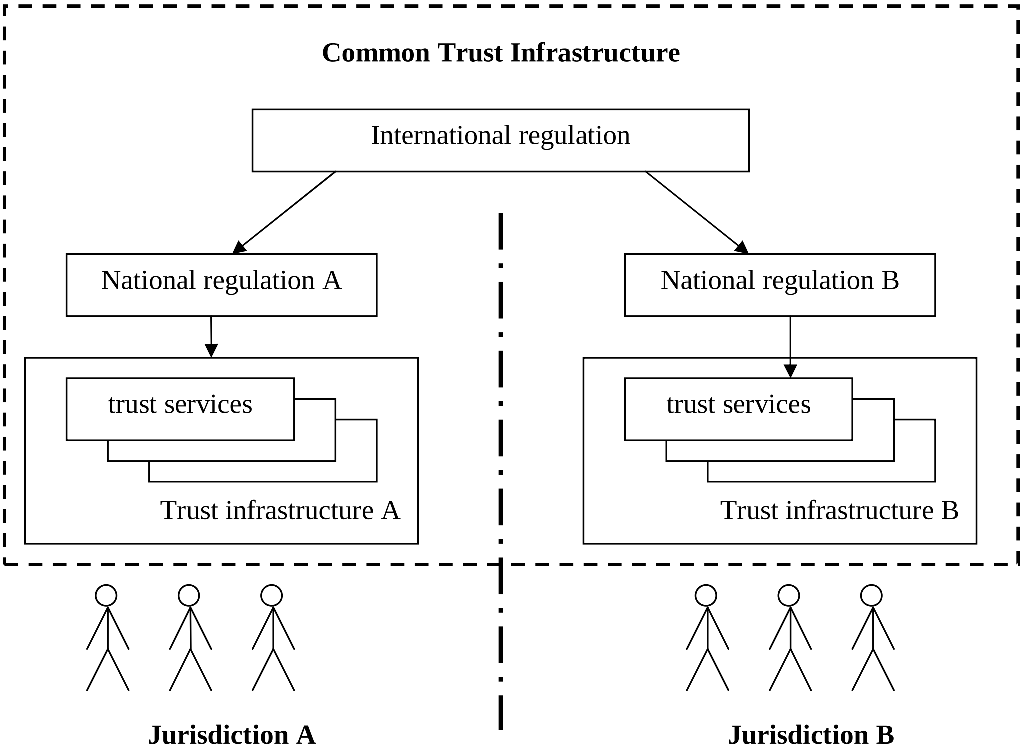

Fig.1. Legal level

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 information 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 the effort of this Recommendation concerning the necessary coordination on the legal level, see sec. 2.6.

Organizational level

Mutual legally significant recognition of 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.

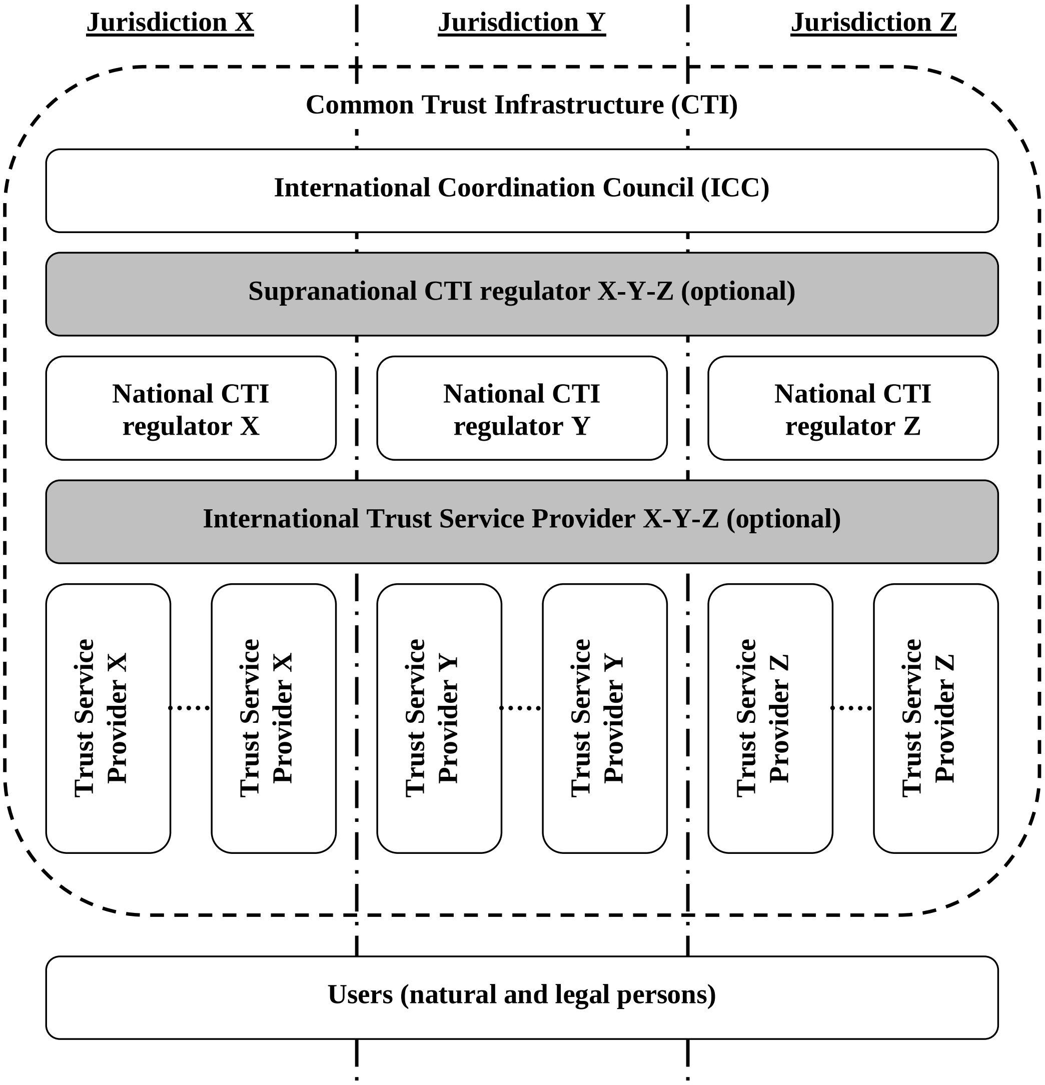

Fig. 2. Organizational level (optional elements are identified by the grey blocks)

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 presented 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 their 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). Thus, 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 the operators of the trust services with respect to their meeting 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, 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 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[3] (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 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.

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

2.4. Trust infrastructures services technical interoperability ensuring approaches

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

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

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

Примечание [s3]: From project proposal

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		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		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 legal entities).

№	Attribute type	Mandatory yes/no	Description/comments
			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		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 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 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

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

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

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

Примечание [s4]: From project proposal

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[4].
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

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

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

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

Примечание [s5]: From project proposal

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;

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

- 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 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.

ANNEX 1

Terms and Definitions[5]

authentication

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

Примечание [AN6]: I agree.

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

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

Код поля изменен

1. The act of verifying identity (i.e., user, system)
Scope Note: Risk: Can also refer to the verification of the correctness of a piece of data

2. The act of verifying the identity of a user and the user's eligibility to access computerized information
Scope Note: Assurance: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.

Примечание [IF7]: This is ‚**authorization**', but not ‚authentication', see below

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

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

authenticity

Примечание [AN8]: –Cf the VAT Directive 2010/45 where in relation to the "authenticity" of an invoice the following is commented: "The supplier must be able to provide assurance that the invoice was indeed issued by him or in his name and on his behalf." –

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

Примечание [IF9]: ‚authenticity' is defined by using ‚authenticity'; it is a dead loop.

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

– Ramachandran:

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

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

Формат: Список

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

3. *Authenticity* is generally understood in law to refer to the genuineness of a document or record, that is, that the document is the “original” support of the information it contains, in the form it was recorded and without any alteration.” Authenticity is the property of being genuine and able to be verified and trusted.

4. *Authenticity* in the electronic environment, further to the high levels of identification, evidentiary and attribution functions may be able to be established through an “authentication framework.” This “authentication framework” would involve legal infrastructure, some technical infrastructure and some organizational infrastructure.

authorization (as a process)

– Eric E Cohen: the approval, permission, or empowerment for someone or something to do something.

Примечание [s10]: Eric E Cohen This is in contrast to when you care not whether the agent is authorized, only that they are who they say they are - authentication. The two are usually considered orthogonal; you normally only wish to check one or the other. I believe in transboundary efforts, authorization is more important than authentication.

– Igor Furgel: approving a subject (a person, an IT component or a process acting on behalf of them) for the execution of a certain action.

certificate

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

Код поля изменен

means a data message or other record confirming the link between a *signatory* and signature creation data.

data unit

a set of digits or characters treated as a whole.

digital certificate

– Aleksandr Sazonov: means a data message or other record confirming the link between a public key (validation data) to a particular distinguished name in the X.500 tradition.

– Igor Furgel: means an electronic attestation which links signature validation data of an entity to the entity and confirms the identity of that entity.

digital signature

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

Код поля изменен

A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation.

A digital signature is generated using the sender’s private key or applying a one-way hash function.

– Igor Furgel (ISO 7498-2 (1989): ‘Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture’):

Data appended to, or a cryptographic transformation of, a *data unit* that allows a recipient of the *data unit* to prove the source and integrity of the *data unit* and protect against forgery, e.g. by the recipient.

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

electronic signature

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

- Eric E Cohen (http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf):

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

  Digital signatures are an example of electronic signatures.

- Igor Furgel:

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

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

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

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

entity

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

genuineness (in IT)

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

  (a) not having been altered from that created by its issuer
  AND
  (b) the identity of its issuer.

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

genuineness (in law)

Примечание [IF11]: This definition is not a full one, there are also other services of electronic signature.
The main services of a signature are (i) perpetuation function (a signature can be verified by anybody later on at any time), (ii) the determinability of the identity of signatory. Additionally, there are warning and consciousness functions.

Код поля изменен

Примечание [IF12]: There is a quite controversial discussion on it.

Код поля изменен

Примечание [IF13]: Not unconditionally an approval, but, generally, a relationship between the signatory and the message

Примечание [AN14]: The UNCITRAL definition is not uncontroversial. We should also look at the new definitions of e-signature and e-seal of the EU EIDAS Regulation, rather than the -99 Directive referenced above.

Примечание [IF15]: The foot note No. 5 in the REC. 14 may also be helpful here:
"In general, signature and authentication in an Information Technology (IT) environment often encompass some inherent functions which can vary from integrity, genuineness, proof, security, etc. Again, all of these terms can have differing interpretation based on environment and geography. This Recommendation has been prepared to align itself with the works of UNCITRAL while remaining consistent with the use of these terms in other UNECE trade recommendations. When reading or drafting any text on the subject, clear identification of which approach is being used, is recommended. For legislators who will probably use a legal definition, reference to UNCITRAL documents on the subject is recommended in order to clearly identify the legal use of these terms. "

– Igor Furgel: (130201+Rec14+survey+on+def_levels+consolidated+responses): "*Authenticity* is generally understood in law to refer to the *genuineness* of a document or record, that is, that the document is the “original” support of the information it contains, in the form it was recorded and without any alteration.” *Authenticity* is the property of being *genuine* and *able to be verified and trusted*".

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

information interaction

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

integrity

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

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

Код поля изменен

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

Примечание [AN16]: Perhaps not always “guarding against” but rather allowing for detection of change.

– Ramachandran:

1. *DATA INTEGRITY*—A condition in which data has not been altered or destroyed in an unauthorized manner

2. *Integrity* is a state of information that assure that it is accurate,complete, consistent and has been protected from errors or unauthorized modification.

Формат: Список

3. *integrity* refers to the resource is untampered with, uncorrupted and complete in all its essential respects after the act of signature is carried out.

levels of access

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

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

levels of authentication

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

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

non-repudiation

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

privacy

Примечание [AN17]: Should we deal with “privacy” or “personal data” rather?

- Eric E Cohen (http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf):

Код поля изменен

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

Примечание [s18]: Eric E Cohen My *personal* interpretation includes information about both individuals (people) *and* organizations.

signatory

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

Код поля изменен

a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents.

Примечание [IF19]: Not just acts, but creates an electronic signature

Примечание [AN20]: Possibly only “creates”, not necessarily ”acts on behalf”.

- Igor Furgel (Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions):

a natural person who creates an *electronic signature*.

time stamp

Удалено: *stamping*

- Eric E Cohen: a trusted indication of when an action, particularly the application of a digital signature, took place.

Примечание [s21]: Eric E Cohen Time stamping is vital in cryptography as people change roles and signatures expire; it is important to know whether the signature was valid and the signer was authorized or could be authenticated at the point of *signing* rather than the point of *checking*.

- Igor Furgel (Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions):

data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

transboundary trust space (TTS)

- Aleksandr Sazonov: a set of normative, organizational and technical conditions for establishing trust in transboundary electronic interaction between public governmental authorities, public non-budgetary funds, local authorities, organizations and citizens.

- Ramachandran: a technological and legal framework for trust establishment in transboundary electronic informational interaction of entities in different legal frameworks’ subjects.

- Eurasian Economic Community Agreement: an aggregate of legal, organizational and technical conditions, harmonized by the member-states in order to ensure trust in international exchange of data and electronic documents between authorized bodies.

trust domain

- Igor Furgel: informational and legal space using the same CTI. A trust domain may also be a single jurisdiction.

trust service provider (TSP)

– A natural o legal person who provides at least one trust service.

what-you-see-is-what-you-sign

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

XML Signature

ANNEX 2

Mathematical description of nIDG functions

- 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