United Nations A/CN.9/WG.III/WP.136*

General Assembly

Distr.: Limited
2 September 2015

Original: English

United Nations Commission on International Trade Law
Working Group III (Online Dispute Resolution)
Thirty-second session
Vienna, 30 November-4 December 2015

Online dispute resolution for cross-border electronic commerce transactions

Submission by the Russian Federation

Note by the Secretariat

The Government of the Russian Federation has submitted to the Secretariat a document containing a vision and conceptual approaches regarding online dispute resolution for cross-border electronic commerce transactions. The document was submitted to the Secretariat prior to an earlier session of Working Group III (Online Dispute Resolution) but it is now to be made available to the Working Group. The text received by the Secretariat is reproduced as an annex to this note in the form in which it was received.

[*] Reissued for technical reasons on 4 November 2015.

Annex

Vision and conceptual approaches to elaboration in specialized United Nations agencies and in relevant international organizations a family of recommendations on establishing and functioning of a trans-boundary trust space

Introduction

"Trans-boundary trust space" (hereinafter — TTS) is proposed to mean a combination of legal, **organizational and technical conditions recommended by relevant specialized United Nations agencies (departments) and** international organizations with the aim of ensuring trust (confidence in authenticity) in international exchange of electronic documents and data between electronically interacting parties (subjects).

"Electronically interacting parties (subjects)" is proposed to mean the entirety of public authorities, physical and legal persons interacting within relations arising from forming, sending, transmitting, receiving, storage and using electronic documents and data.

These proposals purpose to identify approaches and issues to be discussed in the context of development of a set of Recommendations on forming and functioning trans-boundary trust space (TTS Recommendations) in related United Nations organizations. It intends facilitating the building of technical, institutional and legal infrastructure for practical use of the TTS Recommendations.

Interested delegates and experts from state agencies and business are welcome to participate in this discussion.

Possible WTO role and contribution to TTS. The establishing of TTS will contribute to the facilitation and development of international trade and WTO attention to TTS issues will help to mobilize the support from governments and business to its practical implementation. Another area of concern is the lack of a coordination of work (and often of interoperability of final outputs) between numerous international and regional organizations (for example, ISO, ITU, UNECE/CEFACT, UNCITRAL, APEC, etc.) which are working on e-standards and related issues. The assigning to WTO a coordinating role in this process will make the international standardization in this area more efficient and effective.

Conceptual approaches

1. TTS Recommendations are proposed to be aimed 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.

2. The mentioned 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.

3. It is proposed 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 trusted ICT 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 forming and functioning regional and global TTS-clusters as well as for functional services provided in the frames of these clusters are proposed to be considered in a separate UNCITRAL Recommendation.

4. It is proposed to give a description of the possible sets of trusted infrastructural ICT services in conjunction with the criticality of functional applications. The services and their available levels of trust can be determined by the operators of functional information systems dependent on threats, risks, agreed legal regimes and users' demands. In order to ensure required levels of trust the operators of functional information systems can operate in a neutral international environment defined by given legal regimes. It is proposed to describe organizational infrastructures necessary for establishing and maintaining the neutral international environment.

Common provisions on forming and functioning of regional and global TTS clusters, functional services provided in the frames of these clusters as well as sets of trusted infrastructural ICT services can be considered in the UNECE-UN/CEFACT "Recommendation for ensuring legally significant trusted trans-boundary electronic interaction".

Description of single trusted ICT-services can be a subject of technical standards and recommendations ITU, JTC-1, ETSI and others.

5. Sets of identification attributes can be defined by the legal regimes for the business activity of operators specialized in performing identification and functional operators and can be maintained by the related trusted ICT services. Operators' activity can be regulated by special organizational and technical requirements directed, besides others, on personal data protection.

Sets of identification attributes and identification procedures themselves can serve as the basis for the definition of the trust levels of identification schemes. The levels of trust of identification schemes can be of essence for regulation of interaction between different clusters of trust (see item 9).

6. It is proposed to describe the mechanisms of interaction of particular states and their international unions with other international formats in the frames of forming of a common TTS:

6.1. On the basis of accession to an existing legal regime, which ensures institutional guarantees to the subjects of electronic interaction:

- A complete accession of a state to an existing legal regime on the basis of international treaties and/or directly applicable international regulation, in which frames a task on forming a regional TTS has already been set or solved, including functional services provided in the frames of this TTS;

- A partial accession of a state to an existing legal regime on the basis of international treaties and/or directly applicable international regulation, in part of provisions on forming of regional and/or functional TTS;

6.2. On the basis of interaction between different international unions:

- In the first stage, a group of states creates an isolated regional TTS cluster, including functional TTS services provided in the frames of this TTS, ensuring institutional guarantees for the subjects of electronic interaction within the legal regime specified by these states;

- In the second stage, the protocols of trusted interaction with other international unions are specified as related to mutual recognition of different legal regimes. This mutual recognition shall regard to institutional guarantees and information security requirements appertaining to each of the international formats, possibly on the basis of an information security gateway (ISG) being operated in the frames of a special legal regime.

6.3. On the basis of interaction of a state with other states or international unions:

- In the first stage, a state creates an isolated national TTS cluster 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 an information security gateway (ISG) being operated in the frames of a special legal regime.

7. It is proposed to describe cluster-forming mechanisms, similar to item 6, for legal regimes based on commercial agreements and/or common trade practice.

8. It is proposed to describe the mechanisms of forming of a global TTS based on integration of different clusters into a matrix formed according to the following characteristics:

- Functional services and regional scope,

- Different legal regimes and their modifications.

9. It is proposed to describe approaches to forming several types of information security gateways (ISG) as key elements of building a global TTS matrix.

The aim of creation of such gateways can be enabling of interaction between different clusters of the global TTS. Gateways forming can consider all the necessary aspects: legal, organizational and technological.

Approaches to forming typical information security gateways can take into account the existence of different possible levels of interaction between different TTS clusters. In particular, gateways forming can be done both: at only legal and organizational levels and at a complex level: legal, organizational and technical one.

Approaches to forming of typical information security gateways can regard usage of transition profiles describing and configuring transitions from one cluster to another. These transition profiles can consider the trust levels of the identification schemes used inside the interacting clusters, see item 5.

Description of several types of information security gateways (ISG) can be a subject of technical standards and recommendations ITU and JTC-1.

Summary

The problem of trans-boundary exchange of electronic documents is topical and is noted in global and regional declarations, such as:

- Promote research and cooperation enabling effective use of data and software in particular electronic documents and transactions including electronic means of authentication and improve security methods (WSIS+10 Vision for WSIS Beyond 2015, C5. Building confidence and security in the use of ICTs, para. f.).
- Promote confidence and trust in electronic environments globally by encouraging secure cross border flows of information, including electronic documents and efforts to expand and strengthen the Asia-Pacific Information Infrastructure and to build confidence and security in the use of ICT (2012 APEC Leaders’ Declaration, Vladivostok Declaration — Integrate to Grow, Innovate to Prosper).

There are several good practices of solving such a task in the world now:

- In the European Commission — on the basis of the Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (project — eIDAS[1]);
- In the Eurasian Economic Union — on the basis of the Treaty on the Eurasian Economic Union and of the Conception of using services and legally significant electronic documents in interstate informational interaction;[2]
- In the Asia Pacific Region — on the basis of PAN ASIAN e COMMERCE ALLIANCE (PAA).[3]

The global economy development needs, especially in crisis periods, demand an activation of integration processes in different economic and social areas including

[1] http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond.

[2] www.eurasiancommission.org/docs/Download.aspx?IsDlg=0&print=1&ID=5713.

[3] www.paa.net/.

through the use of modern ICT-technologies based on innovations. These are the tasks the family of the TTS Recommendations proposed for development is aimed to solve.

Comment to attention of the experts of Working Group III UNCITRAL "Online dispute resolution — ODR"

The problem of identification of claimants and defendants in ODR can be solved in the context of the above proposed model (the model of forming and functioning of the trans-boundary trust space as a matrix, built of regional and global clusters, connected between each other and including the functional services provided in the frames of this TTS) as follows:

- One organizes a functional TTS cluster specialized in support of ODR procedures as regards to trans-boundary electronic commerce transactions;
- All the United Nations Member States can be involved in this cluster's geography;
- The functioning of this cluster is maintained by the business activity of a specialized operator or a group of related operators;
- The subject of the specialized operators' business activity can be provision of packages of trusted ID-services based on a set of ID-schemes adopted in the frames of electronic trade platforms;
- Legal regime for the specialized operators' business activity shall be established by agreements with trade platforms.

On the basis of the above stated the following amendments to ODR Procedural rules draft are proposed:

Article 4A, paragraph 4 (h) should be reworded as follows:

A signature or other means of identification and authentication of a claimant and/or the claimant's representative as set forth by the UN/CEFACT "Recommendation for ensuring legally significant trusted trans-boundary electronic interaction".

Article 4B, paragraph 2 (g) should be reworded as follows:

A signature or other means of identification and authentication of a defendant and/or the defendant's representative as set forth by the UN/CEFACT "Recommendation for ensuring legally significant trusted trans-boundary electronic interaction".

The addendum to
Vision and conceptual approaches to elaboration in specialized UN agencies and in relevant international organizations a family of recommendations on establishing and functioning of a trans-boundary trust space

Common trust infrastructure for legally significant trans-boundary electronic interaction

White paper

Development purpose

The Internet has become a habitual tool for obtaining electronic services for individuals and entities of various states. The advantages of such services are evident but there is a number of organizational and legal issues, preventing their wide usage in those activity areas where users need a certain level of trust in these services. One of the main issues is **ensuring validity of e documents and legal significance of electronic interaction in general**. This problem is urgent on both the national level — within given jurisdictions, and the trans-boundary one — by interaction of participants relating to jurisdictions of different states. These issues were repeatedly considered at different international forums, including the United Nations (UN/CEFACT, UNCITRAL), as well as on the regional level — in the CIS, EU and APEC. But a satisfactory solution has not yet been found.

In order to enable a trusted trans-boundary electronic interaction, the RCC[4] experts initiated creation of the trans-boundary trust space (hereinafter — the TTS) based on the common trust infrastructure (hereinafter — the CTI). Its **primary objective is to provide trust services of different qualifications (basic, medium, high) to the CTI users in the process of their electronic interaction**. This will make it possible to attach legal significance to an electronic interaction at users' discretion regardless of their location and jurisdiction.

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

In the course of work on the TTS system, the CTI architecture was proposed, interconnections of its different components and their interaction with users were described, with projecting being carried out simultaneously in three aspects: legal, organizational and technological. The analysis of variants of practical realization and scripts of the CTI use allowed creating a list of documents necessary for a complete specification of the system.

The next step in promoting the new product, in our view, could be a discussion of the accumulated experience and knowledge with different partners (experts and organizations) interested in facilitating, simplifying trans-boundary electronic services and at the same time giving them legal validity.

[4] The Regional Commonwealth in the field of communications. www.rcc.org.ru.

There should also be developed sets of normative, organizational and technological documents ensuring the interoperability within the framework of a respective "trust domain"[5] (see chap. 4 § 3).

Further, there are plans to proceed to particular work involving forming the trans-boundary trust space, beginning with creation of international coordination bodies and the CTI architecture within the framework of a respective "trust domain", following which the practical realization of systems of legally significant trans-boundary electronic interaction will start.

Ensuring international trust: CTI Architecture

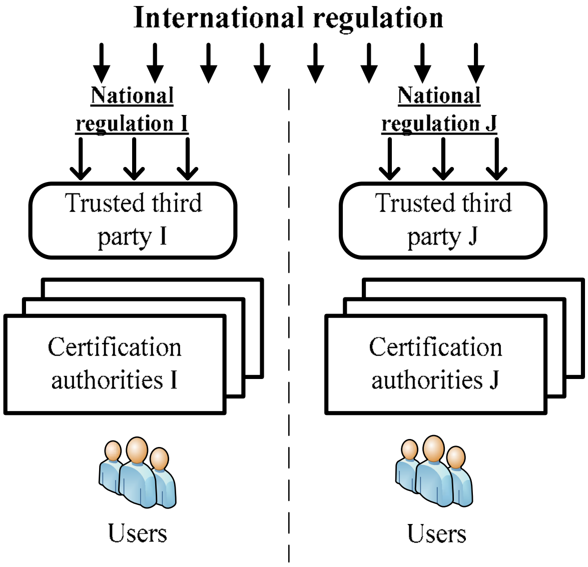
The development of the TTS is being carried out at three levels: legal, organizational and technological. A complex description allows correct functioning of the system as a whole and its single elements.

The CTI architecture is selected 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.

Legal level

The TTS 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. The multi-domain system involves applying means of a trusted third party (hereinafter — TTP). Fig. 1 gives a general scheme of a legal regulation.

Figure 1
Legal regulation of trans-boundary trust space



[5] Information and legal space using the same CTI.

Legal regulation of legally significant trans-boundary information 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 trans-boundary information interaction on given issues;
- Model acts.

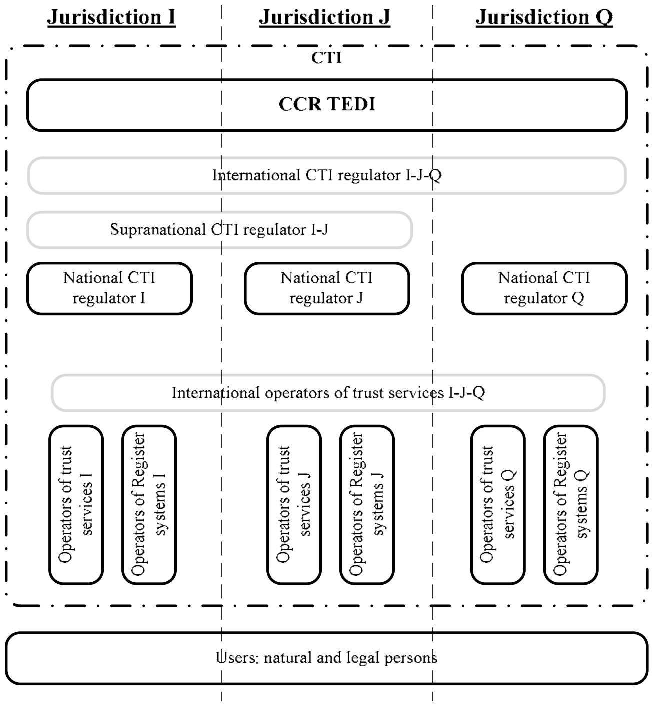
The national legal regulation is built on a complex of normative documents that are standard in each particular jurisdiction.

Organizational level

Mutual legally significant recognition of trust services provided under jurisdiction of various states is reached through creation and operation of the Coordination Council of Regulators of Trusted Electronic Data Interchange (hereinafter — CCR TEDI). The activity of this body is regulated by the CCR TEDI Statute which is to be recognized and signed by all its authorized members — that is the Regulation Bodies of the Electronic Data Interchange represented primarily by the National Regulators of the CTI.

The organizational regulation can be presented by the following diagram (see Fig. 2):

Figure 2
Organizational regulation of the trans-boundary trust space (optional elements are identified by the grey frame)


Jurisdiction I
Jurisdiction J
Jurisdiction Q
CTI
CCR TEDI
International CTI regulator I-J-Q
Supranational CTI regulator I-J
National CTI regulator I
National CTI regulator J
National CTI regulator Q
International operators of trust services I-J-Q
Operators of trust services I
Operators of Register systems I
Operators of trust services J
Operators of Register systems J
Operators of trust services Q
Operators of Register systems Q
Users: natural and legal persons

The CCR TEDI issues a number of documents interconnected with its Statute:

- Requirements for the CCR TEDI members, correspondence to which is a prerequisite for the full membership in the CCR TEDI;
- Guidelines on carrying out "shadow" supervision for admittance to the CCR TEDI and periodic mutual audit for maintaining voluntary membership in the CCR TEDI;
- Compliance criteria which are to be met by operators of the CTI services and operators of the register systems, and the methodology for applying these criteria;
- Scheme of estimation/verification of operators of the CTI services and operators of the register systems with respect to their meeting these criteria.

In the TTS, each jurisdiction is presented by the National CTI regulator (see Fig. 2, National CTI regulators I, J, Q) which regulates the activity of operators of the trust services and operators of the register systems within their jurisdiction.

For groups of states with high degree of integration (for example, EurAsEC or EU) there is the possibility of forming a Supranational CTI regulator (see. Fig. 2, Supranational CTI regulator I J). Thus, one Supranational CTI regulator I-J substitutes a group of National CTI regulators I and J.

The natural CTI scalability is enabled through the procedure for admitting new members to the CCR TEDI (new jurisdictions and supranational participants) and the scheme for verifying the operators of the CTI services and the operators of the register systems with respect to their meeting the Criteria issued by the CCR TEDI (new operators of the services and register systems).

If the CCR TEDI members (see below) have reached conditionally "medium" trust level, they can initiate creation of the International CTI regulator and International operators of the trust services (see. Fig. 2, International CTI regulator I J Q and International operators of the trust services I J Q). The International CTI regulator will coordinate interaction of international operators of the trust services and National CTI regulators (under the CCR TEDI Statute) and/or National CTI regulators.

In order to become a National operator of the trust service or an operator of the register system, a supplier of the respective services shall undergo accreditation with the National CTI regulator of the same jurisdiction. International operators of the trust services shall undergo accreditation with the International CTI regulator. The requirements for accreditation of the operators of the trust services and the operators of the register systems, as well as the requirements to their activity are regulated by the Compliance Criteria issued by the CCR TEDI and possible national supplements issued by the respective regulator.

In the TTS, the users of electronic services can be both individuals and legal entities. The users select the necessary level of trust service qualification at their discretion or in an agreement.

The services are provided by the respective suppliers — the operators of the trust services. In some cases, the services can be provided by the operators of the register systems as well. The operators of the trust services and the operators of the register systems are integrated by the common trust infrastructure.

The trust services as the TTS elements can have different variants of realization depending on the level of trust between the participants of information interaction. For example, with conditionally “high” or “medium” level of mutual trust between the CCR TEDI members, it is efficient to use centralized international 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 services in each state.

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 CCR TEDI documents.

The technological functioning of the trust services can be demonstrated by verification of an electronic signature (hereinafter — ES) in the process of trans-boundary electronic interaction. For comparison, two variants of the CTI realization are given: the decentralized option — at conditionally “low” level of trust between the participants of information interaction (see Fig. 3) and the centralized option at “medium” level of trust between them (see Fig. 4).

Figure 3
ES verification within the framework of the TTS with “low” trust level (decentralized option)

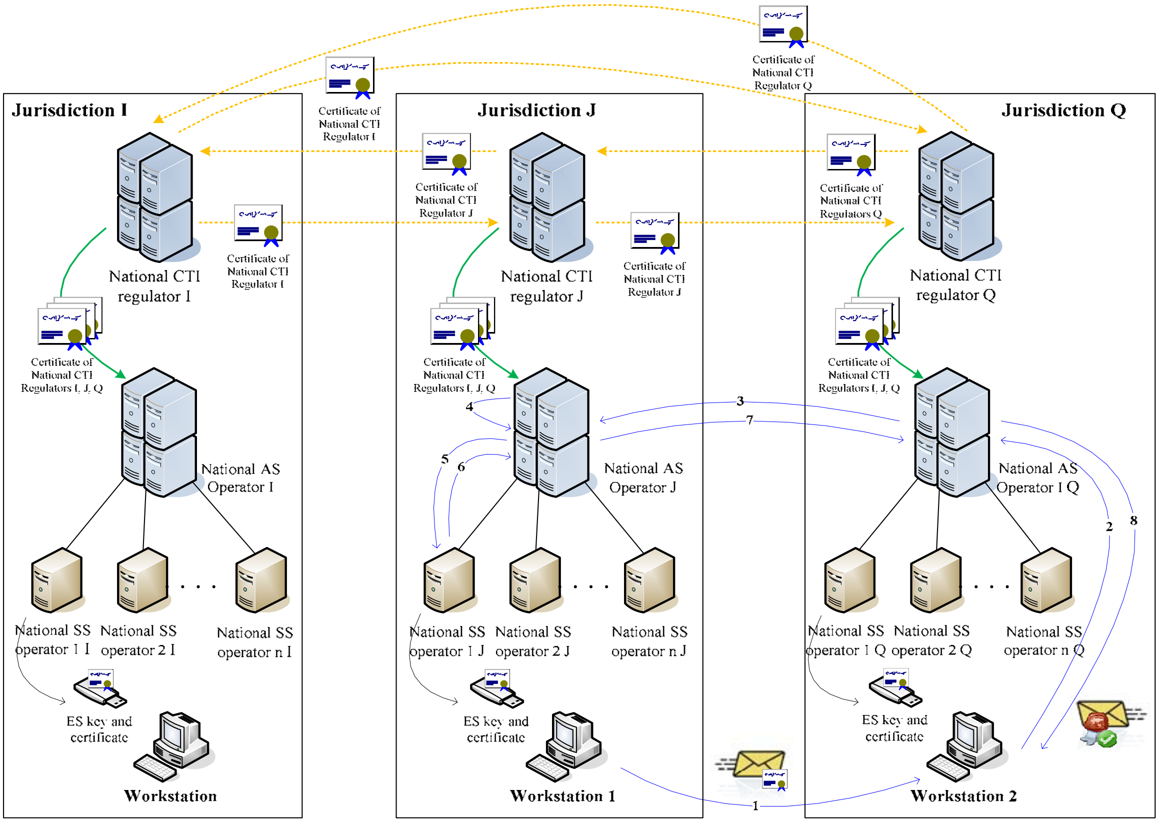


Figure 4
ES verification within the framework of the TTS with “medium” trust level (centralized option)

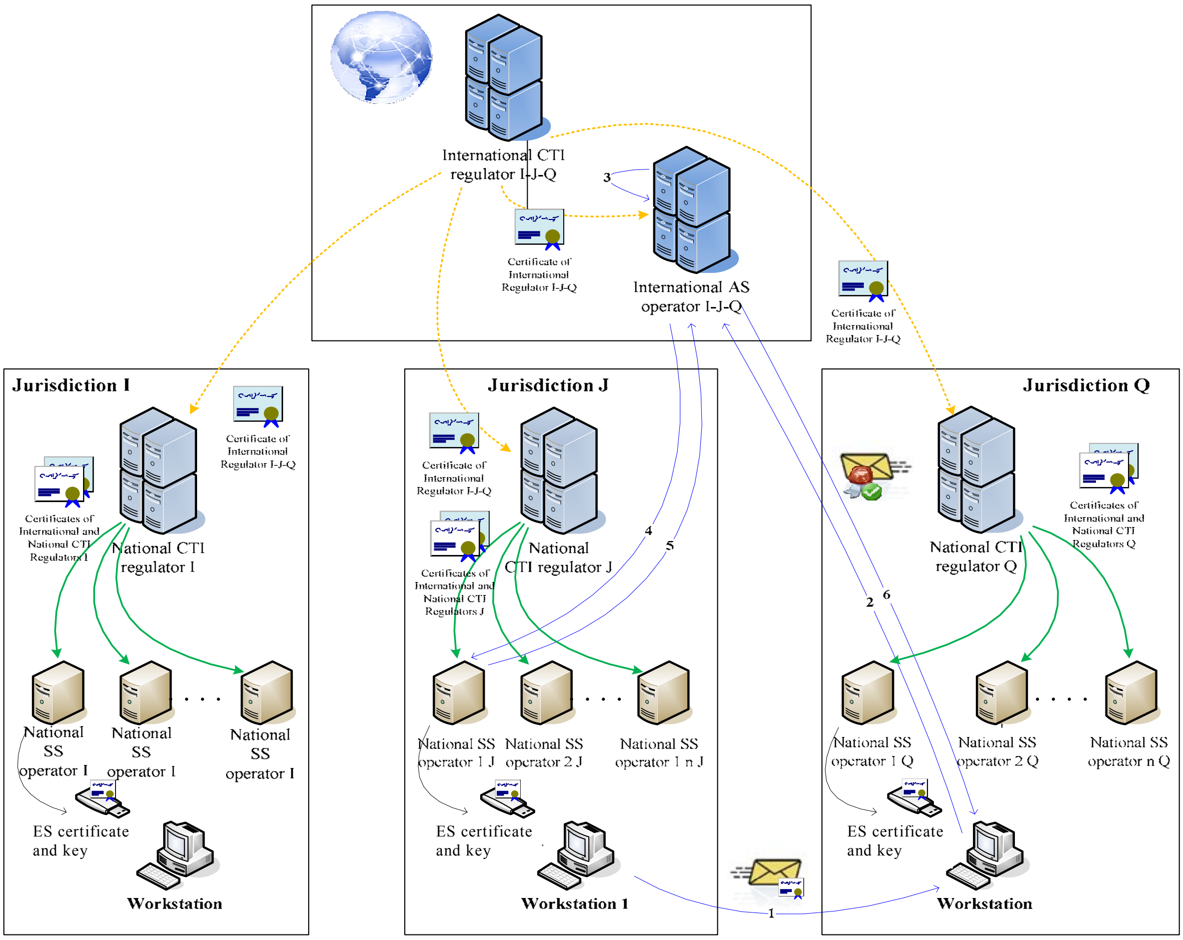

International CTI regulator I-J-Q
3
Certificate of International Regulator I-J-Q
International AS operator I-J-Q
Certificate of International Regulator I-J-Q
Jurisdiction I
Certificate of International Regulator I-J-Q
Certificates of International and National CTI Regulators I
National CTI regulator I
National SS operator I
National SS operator I
National SS operator I
ES certificate and key
Workstation
Jurisdiction J
Certificate of International Regulator I-J-Q
Certificates of International and National CTI Regulators J
National CTI regulator J
4
5
National SS operator 1 J
National SS operator 2 J
National SS operator 1 n J
ES certificate and key
Workstation 1
1
Jurisdiction Q
Certificates of International and National CTI Regulators Q
National CTI regulator Q
2
6
National SS operator 1 Q
National SS operator 2 Q
National SS operator n Q
ES certificate and key
Workstation

Table 1 shows the specifics of the decentralized and centralized CTI options. The ES verification procedure for the two variants of CTI realization is described in Table 2.

Table 1
CTI specifics for information interaction with "low" and "medium" level of trust

Low level of trust (Fig. 3)	Medium level of trust (Fig. 4)
1. Apostille services are provided by the National operators of apostille service (AS). 2. International organizations (operators and regulators) are unavailable. 3. The National Regulators interact directly, exchanging certificates among themselves (⇢). 4. The National Regulators provide the National operators of the trust services belonging to their jurisdiction with their certificate and the certificates of the National Regulators of other jurisdictions (→).	1. Apostille services are provided by the International operators AS. 2. International organizations present: the International CTI Regulator and the International operators of the trust services. 3. The National CTI Regulators interact only through the International CTI Regulator. Likewise, the National operators of the trust services interact through the respective International operator. 4. The International CTI Regulator provides the National operators of the trust services and the National CTI Regulators with the certificates in the centralized manner (⇢). 5. The National Regulators provide the National operators of the trust services belonging to their jurisdiction with their certificate and the International Regulator's certificate (→).

Table 2
Procedure for ES verification for the options with "low" and "medium" level of trust

Low level of trust (Fig. 3)	Medium level of trust (Fig. 4)
1. Individual/entity 1 sends the documents signed with ES in jurisdiction **J**, meanwhile selecting the necessary qualification level of the trust services in use provided by the CTI (basic, medium or high). 2. A request for verifying documents with ES of jurisdiction **J** is forwarded to the National operator of the apostille service (AS) belonging to jurisdiction **Q**. 3. A request for verifying documents is forwarded to the National AS operator belonging to jurisdiction **J**. 4. Mathematic verification of ES of jurisdiction **J** is carried out. 5/6. A request/response concerning certificate status is sent to the National operator of the signature service (SS) of jurisdiction **J**. 7. The National operator of the AS belonging to jurisdiction **Q** receives a receipt on the correctness of the ES of jurisdiction **J**. 8. The National AS operator of jurisdiction **Q** certifies the receipt and forwards it to individual/entity 2.	1. Individual/entity 1 sends the documents signed with ES in jurisdiction **J**, meanwhile selecting the necessary qualification level of the trust services in use provided by the CTI (basic, medium or high). 2. A request for verifying documents with ES of jurisdiction **J** is forwarded to International AS operator **I-J-Q**. 3. Mathematic verification of ES of jurisdiction **J** is carried out. 4/5. A request/response concerning certificate status is sent to the National operator of the signature service (SS) of jurisdiction **J**. 6. International AS operator **I-J-Q** certifies the receipt and forwards it to individual/entity 2.

Identification of claimants and defendants in online dispute resolution

In the context of above mentioned model of forming and functioning of the trans-boundary trust space as a matrix, built of connected between each other regional and global clusters, including the functional services provided in the frames of this TTS, the problem of identification of claimants and defendants in online dispute resolution (hereafter ODR) can be solved as follows:

- One organizes a functional TTS cluster specialized in support of ODR procedures as regards to trans-boundary electronic commerce transactions;
- All the United Nations Member States can be involved in this cluster's geography;
- The functioning of this cluster is maintained by the business activity of a specialized operator or a group of related operators;
- The subject of the specialized operators' business activity can be provision of packages of trusted ID-services based on a set of ID-schemes adopted in the frames of electronic trade platforms;
- Legal regime for the specialized operators' business activity shall be established by agreements with trade platforms.

Further steps

1. The next stage in promoting this development could be a discussion of the accumulated experience and knowledge with different partners (experts and organizations) interested in facilitating, simplifying trans-boundary electronic services and at the same time giving them legal validity.

Among such interested partners can be primarily political and economic.[6] The political formats already partially involved in this work area are both supranational organizations (for example, CIS, APEC, EU, SCO) and bilateral relations between some states. The economic formats interested in achieving this goal can be, for example, respective United Nations structures such as UNCEFACT/UNECE, UNCITRAL (Working groups III and IV), as well as UNECE, EEA, EurAsEC and others.

2. Further, there are plans to proceed to particular work involving forming the trans-boundary trust space, beginning with the creation of an international coordination body (Coordination Council of Regulators of Trusted Electronic Data Interchange (see Fig. 2). This Council shall adopt its Statute and other regulatory documents governing its activity (see chap. 3.2), determine a specific architecture of the Common Trust Infrastructure (CTI), a set of the CTI trust services to be provided and a possible level of their qualification (possibly, depending on jurisdictions of the operators providing these services).

The existing natural peculiarities (historical, cultural, political, economic, technical, etc.) of different world regions can lead to different formats creating "their own"

[6] Other humanitarian formats can also be interested in this product, for example, in the field of law, the Hague conference on private international law, as well as in the area of medicine and education; however, in our view, such organizations are more likely to use the TTS already created than support its new product.

coordination bodies (CCR TEDI) and CTI architectures according to the level of trust within each format and the natural peculiarities mentioned above.

Therefore, we assume that at the initial stages of this project there will not be a single "trust domain" for the whole planet (for example at a level of some United Nations body), but rather several "trust domains".[7]

3. After the CTI architecture is selected (in a respective "trust domain"), it will be possible to proceed to drafting a further set of organizational, normative and technological documents agreed upon within the framework of the CCR TEDI. The systematic character of this document set is determinable by the results in step 2. This way, interoperability within the framework of a respective "trust domain" will be ensured.

International organizations developing and harmonizing standards can make a significant contribution to the support of these projects.

4. Adopting this set of documents by the CCR TEDI members (in a respective "trust domain") will make it possible to proceed to the final stage of implementation of the systems of legally significant trans-boundary electronic interaction.

[7] Informational and legal space using the same CTI.