United Nations A/CN.9/WG.IV/WP.141

General Assembly

Distr.: Limited
30 January 2017
English
Original: Russian

United Nations Commission on International Trade Law
Working Group IV (Electronic Commerce)
Fifty-fifth session
New York, 24 -28 April 2017

Legal issues related to identity management and trust services

Note by the Secretariat

The Russian Federation submitted to the Secretariat a paper for consideration at the fifty-fifth session of the Working Group. The text received by the Secretariat is reproduced as an annex to this note.

Annex

Proposal by the Russian Federation

Improving the identity management system through use of a transboundary trust environment and a common trust infrastructure for cross-border electronic transactions

Introduction

The Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific was adopted on 24 May 2016 at the seventy-second session of the Economic and Social Commission for Asia and the Pacific (ESCAP).

The objective of the Framework Agreement is "to promote cross-border paperless trade by enabling the exchange and mutual recognition of trade-related data and documents in electronic form and facilitating interoperability among national and subregional single windows and/or other paperless trade systems, for the purpose of making international trade transactions more efficient and transparent while improving regulatory compliance."

Article 5 of the Framework Agreement establishes "improving transboundary trust environment" (paragraph 1 (g)) as one of the general principles guiding the Agreement.

This document is aimed at continuing the work of improving the transboundary trust environment in electronic commerce (e-commerce), an important agenda item for ESCAP and for the United Nations Commission on International Trade Law (UNCITRAL).

An earlier version of the proposal, contained in document A/CN.9/WG.III/WP.136, was submitted to UNCITRAL Working Group III (Online Dispute Resolution) for consideration at its thirty-second session in Vienna (30 November-4 December 2015). On the recommendation of Working Group participants, the document was transmitted to Working Group IV (Electronic Commerce) for consideration owing to its relevance to that Working Group's agenda. The main areas of focus are the technical, organizational and legal mechanisms for strengthening the transboundary trust environment for e-commerce in the Asia and the Pacific region. At the fifty-third session of Working Group IV, the delegation of the Russian Federation expressed its intention to submit a proposal on identity management for the consideration of the Working Group at its next session, subject to confirmation by the Commission that identity management would be included on the agenda of the Working Group at that session. Delegations were invited to submit information on identity management with a view to facilitating consideration of the topic.

Ensuring the security of the cross-border exchange of electronic documents is a highly relevant issue that has been highlighted in global and regional declarations, specifically:

- “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. (World Summit on the Information Society document “WSIS+10 Vision for WSIS Beyond 2015. C5. Building confidence and security in the use of ICTs”, subparagraph (f));
- “[…] promoting confidence and trust in electronic environments globally by encouraging secure cross-border flows of information, including electronic

documents[, and promoting] efforts to expand and strengthen the Asia-Pacific Information Infrastructure and to build confidence and security in the use of ICT" (Vladivostok Declaration (Asia-Pacific Economic Cooperation (APEC) leaders' declaration, 2012): "Integrate to Grow, Innovate to Prosper").

Worldwide, there are currently several examples of good practice in addressing the issue:

- In the European Commission: on the basis of Regulation (EU) No. 910/2014 of the European Parliament and the Council of the European Union on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation);[1]
- In the Eurasian Economic Union: on the basis of the Treaty on the Eurasian Economic Union and the Framework for the use of services and legally significant electronic documents in inter-State informational interaction;[2]
- In the Asia and the Pacific region: on the basis of the Pan-Asian e-commerce Alliance (PAA).[3]

The development of the global economy requires, particularly in times of crisis, enhanced integration processes in various economic and social areas, including through the innovative use of current information and communications technologies (ICT).

One of the main issues that arises with respect to cross-border trade is the security and confidentiality of information transmitted via the Internet. An identity management (IdM) system is used to address that issue. IdM is a set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

- Assurance of identity information (e.g., identifiers, credentials, attributes);
- Assurance of the identity of an entity (for example: users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects); and
- Supporting business and security applications.[4]

The objectives of IdM are:

- Access control (hardware should be accessed only by authorized users and for the purposes that the owners intend);
- Confidentiality of access;
- IdM system integrity.

In order to achieve those objectives, an IdM system should:

- Ensure the necessary system performance with established resilience indicators;
- Ensure the function of identification data management (creation, alteration, freezing, archiving or deletion of identification information);
- Ensure the protection of identification data;

[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/.

[4] https://www.itu.int/rec/T-REC-X.1252-201004-I/en.

- Ensure the use of secure identification and authentication mechanisms (such as an electronic signature, two-step password protection and biometric authentication);
- Ensure the interoperability of the security solutions used;
- Ensure the integrity of the IdM system and of identification information.

There are two types of IdM system: application-centric and user-centric.[5]

In large-scale IdM systems, the application-centric IdM system means that identity services and policies are designed to satisfy requirements for identity providers and optimized for the requirements of applications, e.g. provisioning a user's account information. There is an identity provider and a relying party in the application-centric IdM system. When an identity service is provided for the user, the identity exchange usually takes place between these two entities. “Identity” should be understood as the representation of an entity in the form of one or more information elements which allow the entity or entities to be sufficiently distinguished within context. For IdM purposes the term “identity” is understood as contextual identity (subset of attributes) i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts. Historically, the identity and access management technologies have focused mainly on the authentication of end users for federated access to applications and services (in the federated access model there are multiple identity providers that can be trusted by a user and that can manage the partial identity information of users if required. Identity information of the user in each identity provider can be shared). Therefore, the security requirement is limited to the perimeter of its application domains.

The user-centric IdM is mainly focused on end users and optimized for the requirement of those end users. It means that the main objective of an IdM system is to provide convenient and comprehensive identity services for users. The main feature is to give the user full control over his identity. When a user's identity information is disseminated, it must pass through the user to give the user a chance to enforce some personal policy if necessary; for example, a choice of personal preferences in relation to confidentiality or personal authorization. In the user-centric IdM system, a client program that interacts with the IdM server to retrieve identity information has to be installed in the user's computing environment, Therefore, easy and comprehensive security guidelines are required to guide the user to securely install and deploy any relevant software. The software must manage some of the user's security-related information. User-centricity distinguishes itself from other models of IdM by emphasizing that the user and not an authority maintains control over how a user's identity attributes are created, disseminated, updated and terminated. It means that the user has full authority for the life cycle of their identity. The level of control can be determined by the user's privacy requirements.

IdM issues were first considered within the framework of the International Telecommunication Union (ITU) and its Telecommunication Standardization Sector (ITU-T) in 2006, when the Focus Group on Identity Management was established by ITU-T Study Group 17, which works on telecommunication and ICT security issues. The objective of the Focus Group was to consider IdM questions and common principles in telecommunications and ICT. The Focus Group’s activities evolved into an ITU global IdM initiative which was implemented in 2008. Study groups 2, 9, 11, 13, 16 and 17 of ITU-T collaborated on this initiative. The Joint Coordination Activity for Identity Management (JCA-IdM) has been led by Study Group 17 since 2009. Through the Activity, a road map of IdM standards has been developed, which

[5] https://www.itu.int/rec/T-REC-X.1253-201109-I/en.

includes relevant input by the following organizations: the Alliance for Telecommunications Industry Solutions (ATIS), the European Telecommunications Standards Institute (ETSI),the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ITU, the National Institute of Standards and Technology (NIST), the Organization for the Advancement of Structured Information Standards (OASIS), the Kantara Initiative and the Third Generation Partnership Project (3GPP) (a description of the IdM activities and standards issued by the ITU and these organizations can be found on the ITU website: http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part06.aspx).

The establishment of a transboundary trust environment (TTE) in the area of e-commerce will contribute to the simplification of procedures and to the development of international trade, and will make it possible to simplify the identification process and IdM for participating countries. The term "trust" in the context of security can be understood to mean certainty with regard to the reliability and veracity of information or with regard to the ability and willingness of an entity to act appropriately in a given situation. Creating a trust environment between States will thus help to harmonize the use of security mechanisms (for example, all countries will use a common approach to the selection of such mechanisms as electronic signatures and two-step password protection) and will also make it possible to increase the level of trust (continuing, measurable confidence in the reputation, capabilities, validity or authenticity of someone or something) between participants in e-commerce.

A transboundary trust environment in e-commerce is proposed to mean a combination of legal, organizational and technical conditions recommended by the relevant United Nations specialized agencies and international organizations with the aim of ensuring trust in the international exchange of electronic documents and data between parties (entities) that interact electronically when conducting e-commerce. Its main purpose is to provide users with various levels of trust services (basic, medium, high) with the help of an IdM system during the course of their electronic interaction. This will make it possible for electronic interaction to be given legal significance at users' discretion, regardless of their geographical location and jurisdiction. One of the most important areas of research in this area will be the analysis of possible IdM mechanisms.

It is proposed that "electronically interacting parties (entities)" in e-commerce be understood to mean all public authorities and natural and legal persons interacting within the framework of a relationship resulting from the creation, sending, transmission, receiving, storage and use of electronic documents and data when conducting e-commerce.

These proposals are intended to identify approaches and issues to be discussed in the context of the elaboration of a set of recommendations on the establishment and functioning of a transboundary trust environment (e-commerce TTE recommendations) in relevant United Nations organizations. They are designed to facilitate the establishment of technological, institutional and legal infrastructure for the application of e-commerce TTE recommendations and, in particular, to simplify the IdM system for e-commerce transaction security.

Conceptual approaches

1. It is proposed that e-commerce TTE recommendations be focused on guaranteeing the rights and legal interests of citizens and organizations under the jurisdiction of United Nations Member States in relation to the performance of legally significant information transactions in electronic form using the Internet and other open mass-usage ICT systems.

2. These institutional guarantees would be provided within the framework of the commercial activities of specialized operators that:

- Provide users with a set of trusted ICT services for IdM implementation;
- Operate within the framework of established legal regimes that include, but are not limited to, restrictions concerning personal data processing.

3. It is proposed that a description be given of the various possible legal regimes:

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

Legal regimes can receive additional support from traditional institutions (government bodies, settlement through the courts, risk insurance, notaries public and others) through the mutual recognition of electronic documents authenticated by trusted ICT services.

Established legal regimes may also provide for the introduction of special requirements concerning material and financial support for the commercial activities of specialized operators in case of damage caused by them to users, including instances in which personal data are compromised.

It is proposed that institutional guarantee- and legal regime-related issues with respect to the establishment and operation of regional and global e-commerce TTE clusters and to the functional services provided within the framework of those clusters be addressed in a separate UNCITRAL recommendation.

4. It is suggested that a description be given of possible sets of trusted ICT infrastructure services according to the level of importance of the functional applications. One of the most important areas of research in that regard will be the analysis of possible IdM mechanisms. ICT services and the current level of trust in those services can be determined by functional operators of information systems (operators that organize and/or carry out identity data storage and processing in an information system and that define the objectives and actions (operations) implemented using the identity data in that information system) on the basis of threats, risks, legal regimes and user needs. In order to ensure the necessary level of trust, IdM operators could function in a neutral international environment as defined by specific legal regimes. It is proposed that a description be given of the organizational structures needed in order to establish and maintain such a neutral international environment.

Common provisions on the establishment and functioning of regional and global e-commerce TTE clusters, functional services provided within the framework of those clusters and sets of trusted ICT infrastructure services could be considered within the framework of the United Nations Centre for Trade Facilitation and Electronic Business (CEFACT) and Economic Commission for Europe (ECE) joint "Recommendation for ensuring legally significant trusted transboundary electronic interaction”.

IdM implementation and the description of specific trusted ICT services could be the subject of technical standards and recommendations of ITU, the ISO/IEC Joint Technical Committee 1 (JTC 1), the European Telecommunications Standards Institute and other bodies.

5. Sets of attributes for IdM purposes should be defined by the legal regimes that regulate the commercial activities of operators specializing in performing identification tasks and of functional operators, and can be supported by the

appropriate trusted ICT services. The activities of operators may be regulated by special organizational and technical requirements focused, inter alia, on the protection of personal data.

Sets of attributes for IdM purposes and the identification procedures themselves may serve as the basis for the definition of trust levels in identification systems. Such trust levels could be of the utmost importance in the regulation of interaction between different trust clusters (see section 9).

6. It is proposed that descriptions be provided of the interaction mechanisms of individual States and their international alliances with other international bodies within the framework of establishment of a common e-commerce TTE:

6.1. On the basis of accession to an existing legal regime that provides institutional guarantees to electronically interacting entities:

- The complete accession of a State to an existing legal regime on the basis of international treaties and/or directly applicable international regulations in which the establishment of a regional e-commerce TTE, including functional services provided in that e-commerce TTE, is either envisaged or provided for.
- The partial accession of a State to an existing legal regime on the basis of international treaties and/or directly applicable international regulations through the adoption of specific provisions relating to the establishment of a regional and/or functional e-commerce TTE;

6.2. On the basis of interaction between various international alliances:

- In the first phase, a group of States creates an isolated regional e-commerce TTE cluster, including functional e-commerce TTE services provided within the framework of that TTE, providing institutional guarantees for electronically interacting entities under the legal regime specified by those States and ensuring the security of e-commerce transactions;
- In the second phase, the protocols and mechanisms for trusted interaction with other international alliances are defined in relation to the mutual recognition of different legal regimes. Such mutual recognition should take into account the institutional guarantees and information security requirements relevant to each of those international bodies, possibly on the basis of information security gateways (ISG) operating under special legal regimes and responsible for IdM;

6.3. On the basis of interaction between a State and other States or international alliances:

- In the first phase, a State creates an isolated national e-commerce TTE cluster operating under a national legal regime determined by that State;
- In the second phase, the protocols for trusted interaction with other States and/or international alliances are defined in relation to the mutual recognition of different legal regimes. Such mutual recognition should take into account the institutional guarantees and information security requirements relevant to those States and international bodies, possibly on the basis of ISGs operating under special legal regimes and responsible for IdM.

7. It is proposed that a description be given of cluster-forming mechanisms, similar to those described in section 6, for legal regimes based on commercial agreements and/or common trade practice.

8. It is proposed that a description be given of the mechanisms for establishing a global e-commerce TTE on the basis of integration of the various clusters into a single matrix constructed according to the following parametric input information:

- Types of functional services and regional scope;

- Types of legal regimes and their variants.

9. It is proposed that a description be given of approaches to the establishment of several types of ISG as key elements of building a global matrix for an e-commerce TTE in order to ensure the security of e-commerce transactions.

Ensuring that the conditions for interaction between different global e-commerce TTE clusters are met and that that interaction is secure could be one of the objectives of establishing such ISGs. All the necessary technological, organizational and legal aspects could be considered when establishing the ISGs.

Approaches to establishing generic ISGs should take into account the various possible levels of interaction between different e-commerce TTE clusters. The establishment of ISGs that perform IdM, for example, can be achieved either at the legal and organizational levels alone or at a more complex level: legal, organizational and technological.

Approaches to establishing generic ISGs should take into account the use of transition profiles that describe and define the transition from one cluster to another. Such transition profiles could take into account the level of trust in the identification systems used within interacting clusters (see section 5).

A description of several types of ISG could be the subject of ITU and JTC-1 technical standards and recommendations.

Establishing an e-commerce TTE through a unified trust infrastructure

As stated above, the main objective in establishing an e-commerce TTE is to provide users with various levels (basic, medium and high) of trust services with the help of an IdM system during the course of their electronic interaction.

The e-commerce TTE is a fundamental, easily scalable platform that provides unified and secure access to electronic trust services by using IdM. Since existing electronic IdM systems and mechanisms are taken into account, it is expected that any requirements for the upgrading of those systems and mechanisms in order for them to be included in the e-commerce TTE would be minimal.

During the development of the e-commerce TTE system, a common trust infrastructure (CTI) architecture was proposed, the interconnections between its various components and their interaction with users were described and work was simultaneously carried out in three areas: technological, organizational and legal. An analysis of options for practical implementation and scenarios for CTI use made it possible to produce a list of the documentation required for a complete specification of the system. The CTI architecture was designed in such a way that it would be easy to adjust to scale. It can be expanded easily at any level through the addition of new components, such as new legal systems, new supranational participants or new operators of trust and identity data services.

Technical and technological aspects of the CTI

There may be many technological mechanisms for IdM and trust service delivery. The main requirement applicable to CTI elements is that they ensure interoperability. Regulation at this level would be facilitated by various standards and instructions, as would be provided for by the documentation of a coordination council of regulators of trusted electronic data interchange (CCRTEDI). The use of an IdM mechanism such as an electronic signature in transboundary electronic interaction is an example of the technological operation of trust services. For comparison, two CTI implementation options are given: a decentralized system with a notionally low level of trust between the participants in informational interaction (see figure 1) and a centralized system with a medium level of trust between those participants (see figure 2).

Table 1 sets out the features of the decentralized and centralized CTI systems. The procedure for using an electronic signature as an IdM system mechanism for the two CTI implementation schemes is described in table 2.

Table 1
Use of an IdM mechanism in a CTI for informational interaction, with low and medium trust levels

Low trust level (figure 3)	Medium trust level (figure 4)
1. Apostille services (AS) are provided by national operators of apostille services. These operators may also provide other IdM services. 2. International organizations (operators and regulators) are not involved. 3. National regulators interact directly, exchanging security certificates. ⇢ 4. National regulators ensure the operation of national trust service operators in their jurisdiction with regard to their certificates and those of national regulators under other jurisdictions. →	1. Apostille services (AS) are provided by international operators of apostille services. These operators may also provide other IdM services. 2. International organizations are involved: an international CTI regulator and international trust service operators. 3. National CTI regulators communicate only through the supranational CTI regulator. National trust service operators also communicate only through their respective international operators. 4. The international CTI regulator provides centralized certification of national trust service operators and national CTI regulators. ⇢ 5. National regulators ensure the operation of national trust service operators in their jurisdiction with regard to their certificates and the international regulator's certificates. →

Table 2
Procedure for the use of electronic signatures as an IdM system mechanism in schemes with low and medium trust levels

Low trust level (figure 3)	Medium trust level (figure 4)
1. Natural/legal person I sends documents with an electronic signature (ES) in jurisdiction J, selecting the required level of trust services provided by the CTI (basic, medium or high). 2. A request to verify the electronically signed documents in jurisdiction J is sent to the national apostille service operator under jurisdiction Q. 3. The verification request is forwarded to the national apostille service operator under jurisdiction J. 4. The mathematical verification of the electronic signature is carried out in jurisdiction J. 5/6. A request/response regarding the certificate status is sent to the national signature service (SS) operator under jurisdiction J. 7. The national apostille service operator under jurisdiction Q receives confirmation that the electronic signature is correct within jurisdiction J. 8. The national apostille service operator under jurisdiction Q certifies the request and forwards it to natural/legal person 2.	1. Natural/legal person I sends documents with an electronic signature (ES) in jurisdiction J, selecting the required level of trust services provided by the CTI (basic, medium or high). 2. A request to verify the electronically signed documents in jurisdiction J is sent to the international apostille service operator I-J-Q. 3. The mathematical verification of the electronic signature is carried out in jurisdiction J. 4/5. A request/response regarding the certificate status is sent to the national signature service (SS) operator under jurisdiction J. 6. The international apostille service operator I-J-Q certifies the request and forwards it to natural/legal person 2.

Fig. 1

Electronic signature verification within the framework of a TTE with a low trust level (decentralized option)

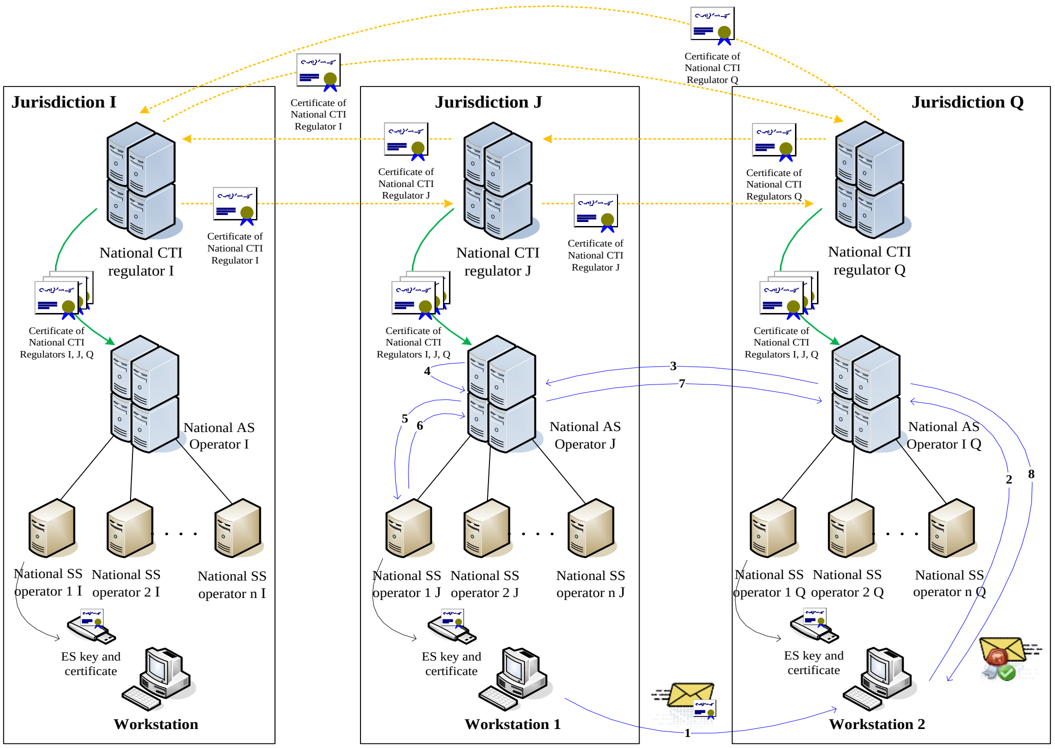
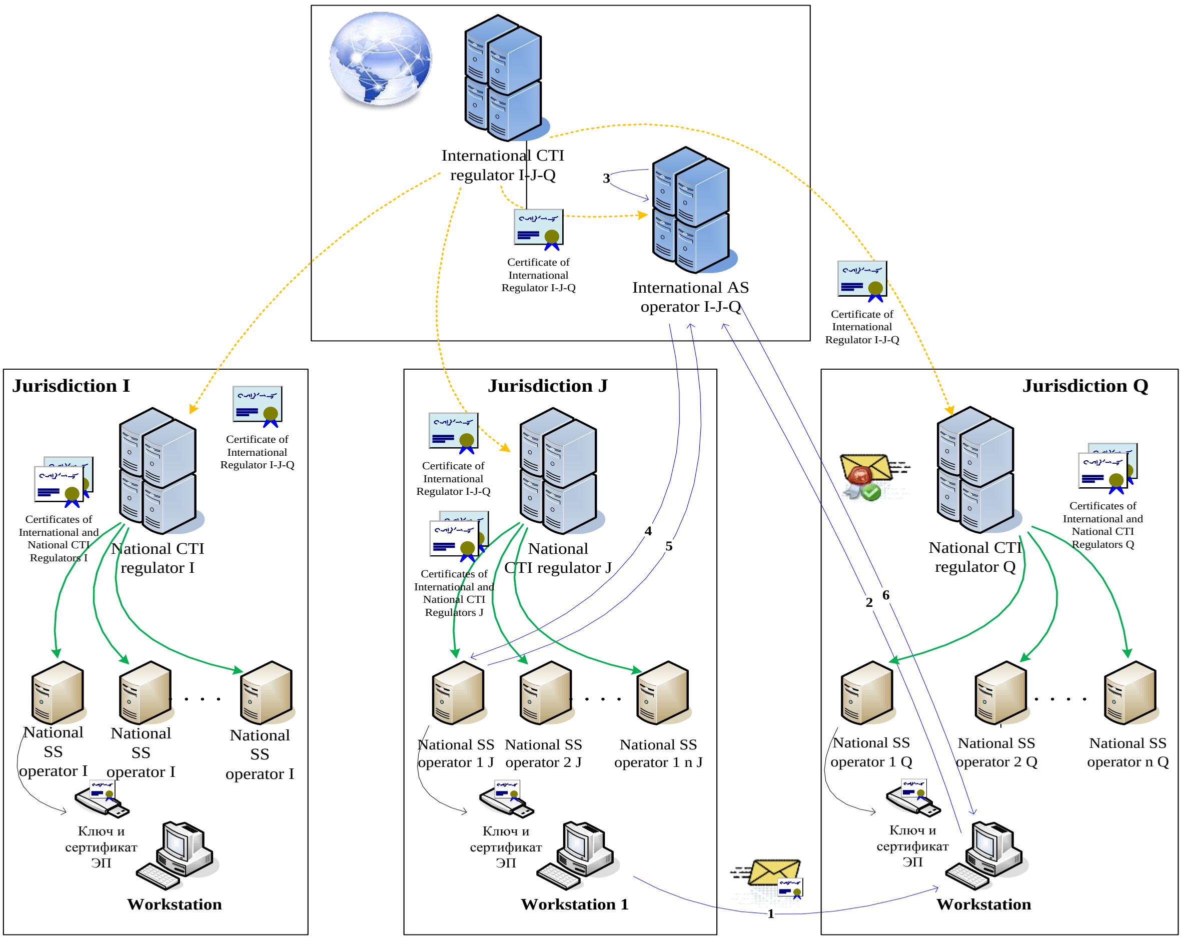


Fig. 2

Electronic signature verification within the framework of a TTE with a medium trust level (decentralized option)

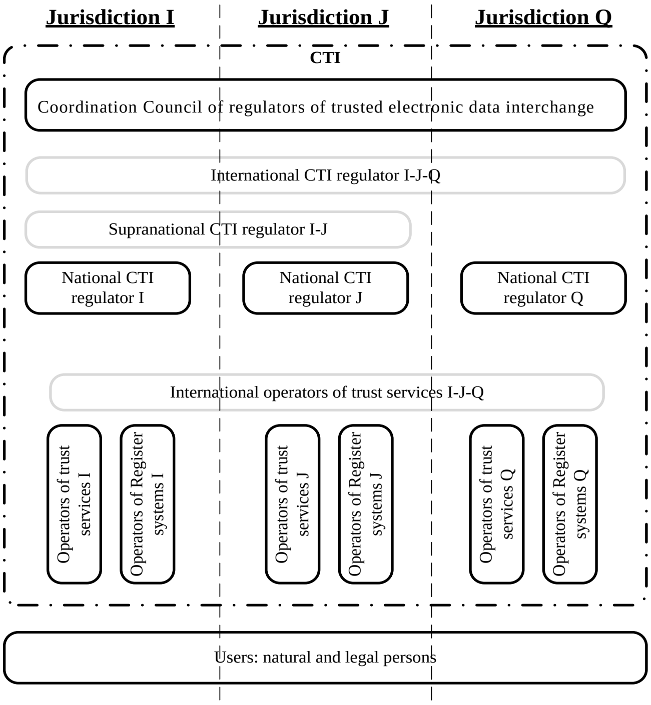

International CTI regulator I-J-Q
3
Certificate of International Regulator I-J-Q
International AS operator I-J-Q
Certificate of International Regulator I-J-Q
Jurisdiction I
Certificate of International Regulator I-J-Q
Certificates of International and National CTI Regulators I
National CTI regulator I
National SS operator I
National SS operator I
National SS operator I
Ключ и сертификат ЭП
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
Ключ и сертификат ЭП
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
Ключ и сертификат ЭП
Workstation

Organizational aspects

Mutual legal recognition of IdM and trust services provided under the jurisdictions of various States would be achieved through the establishment and operation of a coordination council of regulators of trusted electronic data interchange (CCRTEDI). The activities of such a coordination council would be regulated by its statutes, which would be recognized and signed by all its authorized members, that is, the bodies responsible for regulating electronic data interchange, represented in the first instance by national CTI regulators.

Organizational regulation is illustrated in the following diagram (see figure 3):

Fig. 3
Organizational regulation of the transboundary trust environment
(optional elements are indicated by the grey text boxes)


Jurisdiction I
Jurisdiction J
Jurisdiction Q
CTI
Coordination Council of regulators of trusted electronic data interchange
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 coordination council would issue a set of documents, its power to do so being enshrined in its statutes:

- Requirements for coordination council members, compliance with which would be a prerequisite for full membership of the coordination council;
- Guidelines for conducting preliminary “shadow” supervision for admission to the coordination council and periodic mutual audits in order to maintain voluntary membership;
- Compliance criteria for CTI service operators and for IdM and trust service operators, and the methodology for applying those criteria;
- A system for assessing/verifying the compliance of CTI service operators and IdM and trust service operators with those criteria.

In an e-commerce TTE, each legal system is represented by a national CTI regulator (see figure 3, national CTI regulators I, J and Q), which regulates the activities of trust service and IdM operators within its jurisdiction.

It is likely that closely integrated groups of States (such as the Eurasian Economic Community or the European Union) would establish a supranational CTI regulator (see figure 3, “Supranational CTI regulator I-J”). A single supranational CTI regulator I-J would therefore replace the group of national CTI regulators I and J.

The procedure for admitting new members to the coordination council (new legal systems and supranational participants) and the system for verifying the compliance of CTI service and IdM operators with the criteria published by the coordination council (for new operators of IdM and trust services) give the CTI natural scalability.

If members of the coordination council (see below) have achieved a nominally “medium” level of trust, they can initiate the establishment of an international CTI regulator and international IdM and trust service operators (see figure 3, “International CTI regulator I-J-Q” and “International operators of trust services I-J-Q”). The international CTI regulator would coordinate interaction among international trust service operators, national CTI regulators (under the coordination council statutes) and/or supranational CTI regulators.

In order to become a national trust service operator or register system operator, a provider of those services would have to obtain accreditation through the national CTI regulator in the same State. International trust service operators would be required to obtain accreditation through the international CTI regulator. The accreditation requirements for trust service and register system operators and the requirements applicable to their activities would be regulated by compliance criteria published by the coordination council and possibly by national supplements issued by the appropriate regulator.

Both natural and legal persons may be users of electronic services within the framework of the e-commerce TTE. Users would select the required level of trust service at their discretion or by agreement.

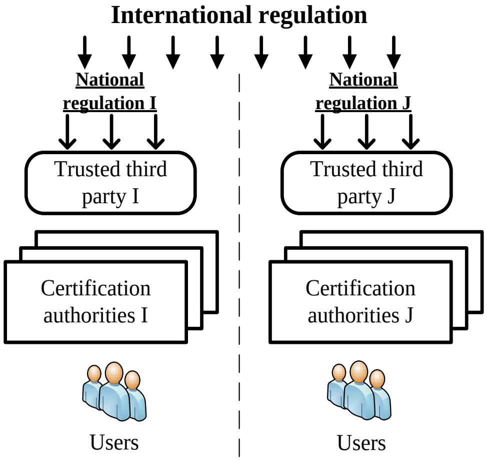
The services would be provided by the appropriate trust service providers/operators. In some cases, services may also be provided by register system operators. Trust service and register system operators would be united by a common trust infrastructure.

There may be various implementation options for trust services forming part of the e-commerce TTE, depending on the level of trust between participants in informational interaction. For example, at nominally high and medium levels of mutual trust between members of the coordination council, centralized international services provided in accordance with agreed standards may be used effectively. In the case of a nominally low trust level, the provision of trust services would be organized according to the principle of decentralization, that is, on the basis of national services in each State.

Legal aspects

An e-commerce TTE can be constructed on the basis of a single domain or multiple domains. A multi-domain basis is the more complex option from a legal and organizational point of view. A multi-domain system requires the use of the technical resources of a trusted third party. Figure 4 shows a general schematic representation of legal regulation.

Fig. 4
Legal regulation of the transboundary trust environment



The legal regulation of transboundary informational interaction can be divided into two parts: international and national. International legal regulation would be carried out on the basis of the following types of document:

- International treaties/agreements;
- Instruments of various international organizations;
- International standards and rules;
- Agreements between participants in transboundary informational interaction on specific issues;
- Model legislation.

National legal regulation would similarly be based on a set of regulatory instruments specific to each individual legal system.

Summary

The material presented above shows that the establishment of an e-commerce TTE offers the optimal means of enhancing the IdM system, for the following reasons:

- The establishment of national, regional and international trust clusters would ensure greater interoperability of IdM mechanisms such as electronic signatures;
- Mutual legal recognition of IdM and trust services provided under the jurisdiction of various States would make it possible to formulate a common approach to IdM system standardization;
- The adoption of international treaties and agreements and international standards and regulations on the use of a TTE would make it possible to enhance the trust level of participants in e-commerce, which in turn would make it possible to simplify IdM implementation;
- The activities of the coordination council (CCRTEDI) would make it possible to draw up unified compliance criteria to be met by IdM and trust service operators, and the methodology for applying those criteria.

IdM system improvement would in turn create secure conditions for transboundary international commercial activities. The establishment of an e-commerce TTE requires the implementation of a number of system-related measures, namely:

- The implementation of technical solutions to ensure the security and confidentiality of information;
- The implementation of organizational solutions through the establishment of a coordinating body;
- The implementation of legal and regulatory solutions through the drawing up of international treaties on the use of an e-commerce TTE.

The organization of an e-commerce TTE will also require coordination among organizations whose work involves issues relating to IdM and cross-border trade (including ISO, ITU, CEFACT, ECE, UNCITRAL and APEC) with a view to developing a common approach both to standardization of the use of an e-commerce TTE as an IdM mechanism and to the use of an e-commerce TTE for transboundary electronic interaction and commercial activities.

The next step in moving this process forward would be the discussion of experience and expertise with various partners (experts and organizations) interested in facilitating, simplifying and at the same time giving legal effect to transboundary electronic services.

Such interested partners might in the first instance be political or economic organizations.[6] Political bodies already partially involved in work in this area include both supranational organizations (such as the Commonwealth of Independent States (CIS), APEC, the European Union and the Shanghai Cooperation Organization) and bodies established within the framework of bilateral relations between certain States. Economic bodies interested in achieving that goal include, for example, the relevant United Nations bodies, such as CEFACT, ECE, UNCITRAL (Working Groups III and IV), ECE, the European Economic Area and the Eurasian Economic Community. It can be assumed that, owing to the specific natural characteristics (including the historical, cultural, political, economic and technical characteristics) of the various regions of the world, various international or regional organizations of countries will establish their own coordination bodies (coordination councils of regulators of trusted electronic data interchange) and CTI architecture, depending on the level of trust within each format and the aforementioned characteristics.

We therefore believe that during the initial stages of implementation of this project there will not be a single global “trust domain” (for example, at the level of one of the United Nations organizations), but rather several trust domains at the regional level or even at the country level.[7] Nonetheless, even the establishment of separate trust domains would improve the IdM system, given the need to ensure interoperability within trust domains.

Once the CTI architecture has been determined (in the relevant trust domain), work can begin on the drafting of a further set of organizational, regulatory and technical documents negotiated within the framework of the coordination council. Interoperability would thus be ensured within the framework of the relevant trust domain.

The adoption of that set of documents by coordination council members (in the relevant trust domain) would facilitate transition to the final stage of practical implementation of the systems for legally significant transboundary electronic interaction.

Comments for the attention of the experts of UNCITRAL Working Group IV on Electronic Commerce

The problem of ensuring security and the identification of entities and objects in e-commerce can be addressed through the model proposed above (model for the establishment and functioning of an e-commerce TTE in the form of a matrix constructed on the basis of interconnected regional and global clusters that include the functional services provided within the framework of that e-commerce TTE) in the following way:

- A functional e-commerce TTE cluster specializing in the creation of a trust zone for IdM in relation to transboundary e-commerce transactions would be established;

- In geographical terms, all United Nations Member States could be included in that cluster;

[6] Other humanitarian organizations may also be interested in this product – for example, in the field of law, the Hague Conference on Private International Law – as well as organizations in the fields of medicine and education; however, in our view, such organizations are more likely to use an established TTE than to support the development of a new product.

[7] An informational and legal environment in which the same CTI is used.

- The operation of the cluster would be ensured through the commercial activities of a specialized operator or group of interlinked operators;
- The provision of packages of IdM trust services based on a set of identification schemes adopted within the framework of e-commerce platforms could be an area of the commercial activities of specialized operators;
- The legal regime for the specialized operators' commercial activities would be established under agreements with e-commerce platforms.