

**Explanatory note
to the Methodology of forming and functioning of
the transboundary trusted space (TTS) in the Internet network**

I. A postindustrial or information society being formed in developed or developing states of the world is a global trend of modernity. One of distinctive information society features is the Internet network, thanks to which significant proportion of the world population has gained breakthrough opportunities concerning access to diverse information and mutual communications. Generally, Internet has brought natural persons and legal entities under jurisdiction of different states nearer to high quality modern business (electronic auctions, logistic support of commodity flows etc), social (telemedicine, distance education etc) and government services. For this purpose, a number of technological, legal and organizational problems are to be solved. They will be referred to and discussed hereinafter, whereas these problems are of both domestic and transboundary nature.

At the same time the world financial crisis made many states start searching for new resources for economic growth, and due to this integration processes gain extra momentum. Forming of common space, harmonic in its economic nature but polycentric from the point of view of particular mechanisms and management decisions can be one of efficient principles in such integration. It seems, that international information systems that are being created, using the Internet network particularly, are to reflect this principle adequately. It implies providing of national segments interoperability taking into account the principle of polycentrism. Traditionally, a field of information security has been one of the most polycentric.

An important factor for smooth solution of the financial crisis is saving of funds at all levels, from states and transnational corporations to common citizens, for whom this factor is crucial. A contradiction between ample opportunities and ever-increasing costs of paper document circulation, that continuously grows and becomes an anachronism, is evident. The latter factor is caused by a general trend in economics and social life globalization, bringing a significant growth of financial, transport, population and service flows clearly seen; a basis to serve the majority of them is an individual document information transaction.

Moreover, an evident contradiction between a limited number of high-grade service (medical, educational, business, etc) providing centers and would-be demand in these services on the part of planet population is witnessed. Direct obtainment of services in such centers involves significant transport and residence costs what excludes low-income strata and, to a greater extent, middle class from

their clientele. At the same time, as an image of such newest services objectively presents in the Internet network, social tension increases in society. Distance providing of services, as a possible solution of this problem, assumes a primary solution of electronic information documentation problems stated above, as well. This is a factor protecting users' and other auxiliary legal relations participants' rights, that has been utilized during centuries in the framework of paper document circulation; with medical history sheets, students' grade books, contracts, etc being spectacular examples of the above-mentioned relations.

Another problem, now in the field of practical implementation of the issues above-stated, is a diversity of state, regional, municipal, corporative and other information systems. Problems of their interoperability provision, at the domestic level, are being solved in the framework of electronic government creation. In connection with the above-stated economic integration trends a crucial issue of interoperability of international information systems national segments is becoming especially important, with the Customs Union Commission (CUC) Integrated Information System of Mutual and Foreign trade (IISMFT) being its working model.

Within this framework, one of such interoperability provision aspects (utilization of electronic signature service) was analyzed in the format of Regional Commonwealth in the field of communications (RCC) of the CIS member states. The dilemma concerned a way of national segments adaptation – either under one of national segments or under some abstract model based on respected international developments, UNCITRAL developments, for instance. Representatives of all the states have voted unanimously for the second, abstract approach, at the same time, it was supposed that any and all the national segments would adopt relative “road maps” on synchronous adaptation in due time (after system design and all the necessary documents drafting and adoption). Such approach was fixed in the Model of CIS Member States TTS Formation and Functioning in the Internet Network, adopted by the CIS Member States Ministers of Communications in Erevan, on June, 2, 2011 (hereinafter referred to as “the TTS Model”). At the same time, further steps were planned, the first one concerns development of Methodology of the TTS Model system design (hereinafter referred to as “the Methodology”), with this document being its first version.

Prior to describing the work performed in the framework of the Methodology it is necessary to point out another principal problem the developers faced. It is as follows. In the framework of traditional delivery of the services considered, for instance – medical and notary, subject content of the service (medical or legal assistance) and documentation of its results are realized by the

same authorized persons, and, speaking more generally, – by the same authorized bodies (organizations). In the example considered they are a doctor and a hospital, or a notary and a notary office. The same relates to government services, which amount to two thousand approximately in Russia at the federal level only.

Conversion of all these services into electronic ones raises the following question – who will provide electronic documentation of the information? Complexity and costs of the infrastructure supporting such documentation are quite significant, besides that, a possibility that it will be impossible to provide interoperability of such private infrastructures, to say nothing of great inconveniences for users, whose number would be commensurate with the world population in case of transboundary service delivery.

All these points dictate an evident decision to separate direct service providers from documentation function and to create a common trusted infrastructure; in its framework a sub-infrastructure of electronic information documentation and a sub-infrastructure of information resources access can be pointed out, since they present the content part of certain services. These sub-infrastructures are designed for implementation of various services, with their description constituting the main content of the Methodology. Besides, synthesis of the decisions gives rise to a number of extra services, with their description being included in the Methodology as well.

Along with evident advantages, a method of electronic information documentation on the basis of the common trusted infrastructure brings about necessity to solve extra serious problems. They emerge due to the fact that a whole aggregation of operators will be responsible for an end service quality and not a single authorized organization (an operator in a general sense). Each of them provides a respective trusted service together with an end content service provider (a doctor, a notary, a public registrar, a customs officer etc). All that implies a distinct delimitation of powers and responsibilities stipulated in a package of unified regulations, development of standardized technological designs, forming a common legal framework.

The above stated problem of the inherited information systems interoperability becomes significantly more complicated in this case and forming some common “assembly point”, with one version of it being proposed and supported by the CIS member states in the framework of the TTS Model, seems to be the only possible solution. At the same time, it seems that each agreed version is a result of compromises anyhow. It testifies that no agreement is perfect. But the fact of a joint agreement becomes extremely important since this is the only way the information systems interoperability sought, can be reached.

Further research and developments in the form of consistent drafting and discussing of the Methodology, of system design and draft documents (organizational, technological and legal) seem to be a possible solution for the complex problem, and practical implementation of a complex engineering-humanitarian system (hereinafter referred to as “the Complex System”).

II. A thesis that the Model approved earlier is a constructive description of the Complex System, a description of the research subject in statics was reflected by the developers in the Methodology. Within this framework, the basis of the entire project is a triune construction consisting of registry systems (RS), electronic transferable records (ETR) and the common trusted infrastructure (CTI). Each element of such a construction is determined through the other two. Developing such description in a dynamic aspect it was possible to recognize some model registry-informational process as being a characteristic feature of all RS. Moreover, RS phenomenology, widely presented in examples but not claiming to be a comprehensive representation, is described in the Methodology as well.

Further, superposition of the Complex system described in its statics/dynamic aspects and existing traditions in sphere of a paper document/document circulation was carried out.

It was stipulated by understanding a necessity to reserve a social function of a document itself in its correct conversion into an electronic analogue. The latter means not only and not just a document in its traditional sense, as a unit (according to the international standard ISO 15489-1—2001 “Information and documentation. Records management. General.”), but the triune info-legal construction described above. At the same time, interpretation of a document in its traditional meaning fits well into the common context of the triune construction as a particular and the simplest case, a stage of an electronic document circulation system development, which will be presented further.

As a result an aggregate of trusted services as a part of above-mentioned documentation and access sub-infrastructures, including some extra services appearing from the common logic of the Complex system composition, was revealed and described. In respect of the TTS Model it means that in any states both RS operators and respective operators of the trusted services are to function. The latter are to provide the transboundary information interaction participants with necessary tools allowing to assign legal validity to the information resources generated in the framework of services being delivered and legally effective in content aspect. The operators of the RS have to ensure security of the information resources contained in these RS. An important factor is that trusted services

realization in the aggregate implies imposing of unified requirements to the RS with their further adaptation in order to provide interoperability.

The Methodology development brought understanding that implementation of each service has a number of options (scripts), technological, first of all. At the same time, different technological scripts imply different information interaction organization and, consequently, different legal support. The whole range of the scripts seemed unlikely to be described and, therefore, it was decided to present for expert consideration the following approach.

Two extreme cases, for the purpose of this discussion called “Light” and “Heavy” for convenience and some intermediate case which could be called “Medium” were taken for consideration. It should be noted at the beginning that the Medium version is plastic and can shift within the limits of Light and Heavy versions. Each of the versions is a set of script implementations of the trusted services, while the description of the extreme cases (Light and Heavy) criteria becomes a key moment.

As it was proposed, the Light version meant the existing level of electronic document circulation systems, implying utilization of departmental and corporate EDMS (generalized name for Electronic Document Management Systems by different manufacturers presenting in the market nowadays) aggregate, as well as traffic environment, as a rule in the form of e-mail, in protected variant, possibly. The e-documents are an electronic version of traditional paper documents (a document as “a unit”) in a standardized file format, for instance PDF, TIFF or another. Document details, such as signature and others can be reproduced electronically, for example on the screen, and printed together with document content. Therefore, interoperability between EDMS and e-mail is performed on the paper document basis, what implies double-circuit scheme – paper and electronic. It is expensive and solves the problem only partially. Nevertheless, such a version is sufficient for a number of cases, which is proved by popularity of such information interaction system. It is clear that within the framework of the Light version different variants exist, for example, utilization of facsimile communication, which seems to be insignificant on methodological level, so far as the principle per se stays important. The details will be required later.

For delimitation of Medium and Heavy versions the following logic is proposed. The implementation of these versions is based on providing of certain trusted services by the respective operators. At the same time, as in the case of the CIS member states or the CUC the key issue is mutual trust between the states participating in transboundary trusted space. One of the main trusted services, electronic signature service, in the both above- mentioned international formats,

was based on the platform of distrust. Therefore, it was decided not to build a centralized PKI-infrastructure, but to use an additional service superstructure over this infrastructure allowing realizing a principle of multi-domain (polycentric) trust that characterizes the opposite decentralized approach (script) to the electronic signature service implementation. In this case, the script of such a service was called a Trusted Third Party (TTP), which corresponds to a narrow interpretation of the adopted term "Trusted Third Party", which in compliance with ITU-T X.842 and RFC 3029 has a broader interpretation. Obviously, in the framework of such approach domestic TTPs have to work according to unified rules – "to be loopback", that is to carry out technological cooperation. A multi-domain trust model based on validation (authentication) of electronic signature and certificates is considerably more complex than traditional hierarchical and browser-based models of PKI trust, used mainly in single-domain PKI-architectures. It is also clear that implementation of the decentralized scheme is significantly more expensive than centralized ones.

Nevertheless, it was a conscious choice in the framework of CIS and the CUC, which seems to be justified for the most crucial trusted service, which is electronic signature utilization. But since the trusted services implementation is not limited to electronic signature only, the issue of other services implementation, their scripts in centralized or decentralized versions appears on the agenda.

Thus, we can note that the Heavy version includes an aggregate of services, with all their scripts having decentralized execution. This is the most complicated and expensive version, theoretically reflecting the maximum degree of distrust between the states participating in the transboundary trusted space. These factors in the aggregate could make it impossible to implement the "Transboundary" project in this or that international format. It turns out that total mutual distrust in the area under consideration is expensive, close to the complexity limit and, perhaps, beyond this limit.

However, other extreme is general complacent trust, which obviously is unacceptable in the modern world either, that is clear without additional comments. Search for "the golden mean", the optimal combination of the principles of centralization/decentralization in trusted services provision is a subject for further consideration in the RCC framework. The developers believe that the present Methodology provides necessary information for reflection and elaboration of solutions on consensus basis. If they are lacking, the further system design could become inefficient.

One of the possible options, in developers' opinion, is the following Medium-version in general. This version implies limitation to the TTP script

decentralized utilization only within the limits of the documentation service and other additional services, while the remaining ones should be implemented in centralized version through the corresponding operator (a set of operators) in one of the CIS member states, for example in Minsk, because the headquarters of the CIS is situated there. Within the access service framework, the centralized issue of accessors should be organized, possibly in Minsk, as well. Meanwhile decentralized personalization should be reserved; including distribution of the accessors to users by domestic competent bodies (organizations), together with issuance of electronic signature private keys based on a domestic certification centers system and providing subjects with the necessary applications.

However, the prerogative of choice is up to CIS member states; for the survey purposes the developers prepared a respective chart, proposed to be filled in foreseeable future, for example by November, 15, 2011. Then the results will be summarized and discussed at the next RCC events.

III. Also, the following topic of crucial significance may be offered for the further discussion. It was revealed during working contacts of Methodology developers with UNCITRAL and CEFACCT representatives and experts, and it is as follows.

Under the current tradition diverse documents exist and we can list just some of them:

- transport or entertainment events tickets;
- passes to various institutions and enterprises;
- official letters, contracts, invoices, other business documentation;
- schemes, drawings, design documentation;
- orders, decrees, ordinances, laws, international treaties, other legal and organizational documents;
- bank notes, promissory notes, shares, other securities and financial instruments;
- variety of other documents, certificates, registration books, journals, files, archival recordings.

There is an individual science dealing with analysis and systematization of this variety of information resources, their circulation (document circulation) – scientific discipline of documentation.

In an information society an issue of document form changing from a paper form to electronic one, reserving a social function of a document per se, is on the agenda. It implies a dialectic solution of the two, generally speaking, opposite problems:

- an electronic form implies the maximum degree of technological solution unification in order to achieve interoperability for the inherited systems and created systems;
- social functions may be different, which is demonstrated by the examples above-shown. Therefore, this empirically formed variety needs to be maximally reserved in technological unification.

There exists some range of solutions for this problem. The Methodology developers propose to consider one of the variants, which is as follows.

A triune information construction, consisting of RS, ETR and CTI, is taken as the TTS Model constructive base. At that we can point out a function priority of the ETR as a social function carrier. The other construction elements are of subordinate, supporting nature:

- RS as a way of ETR organization;
- CTI as a toolbox to assign legal validity to ETR.

Thus, the prevailing meaning of ETR must imply that this category formulated in this particular way is to include organically the whole range of paper document forms and to be a carrier of all possible social functions. That could be achieved if an ETR presents the most complicated case in the whole range of documents/document circulation. It is this position that is contained in many UNCITRAL¹ materials, while an absolutely certain category of documents is meant by ETR².

But while an ETR describes the most complicated case, the other cases can be described via simplifying of this information structure, down to some simplest one. These structures (sub-systems) could be the following:

1. The sub-system description, first of all, includes RS as a centrally maintained register, managed by an operator with regulations and other attributes described by the TTS Model (hereinafter referred to as “the Centralized Register”). E-documents with an off-line status, which are not tightly reserved to one subject of law, could be either issued, or issued, or transferred from one subject of law to another for several times until they become legally ineffective (for example, payment of a promissory note). It is this particular interpretation ETR are used in the above-mentioned UNCITRAL texts. And this is the most complicated case of the system description within the limits of the triune information construction proposed, others are described via simplification. It should be noted that it has not been implemented in practice, which is testified

¹ “Legal issues relating to the use of electronic transferable records”. Note of UNCITRAL Secretariat. Working group IV. A/CN.9/WG.IV/WP.115.

² [1] Section I

by the UNCITRAL efforts to solve this issue somehow. There exists respective correspondence relating to this problem between the Methodology developers and the UNCITRAL and CEFACCT officers and experts. A model analysis of this case is described in Supplement 2 to the Methodology.

2. The sub-system description includes a centralized register, which could issue e-documents with an off-line status, with their tight reservation (for a certain period of time) to one specific subject of law. Such sub-systems can include nearly the whole variety of government services, for instance real estate registration, obtainment of licenses, accreditations, certificates etc. It seems we can claim it is one of the most popular cases.
3. The sub-system description includes only a centralized register, where ETR always have an on-line status. E-documents with the off-line status are prohibited to be issued, with a delimited access being organized to the centralized register. This case is of more theoretical importance, is cited here for completeness of our description and is used for the most crucial RS where the on-line status has the priority significance.
4. The sub-system description does not imply the use of the centralized register. E-documents (messages) are issued by individuals or legal entities and can be transferred to one or several addressees both circularly and in turn. In certain cases they can be accepted as evidence in legal proceedings. It seems that it is exactly the same case described in the UN Convention “On the Use of Electronic Communications in International Contracts” of 2005 and it is quite widespread.
5. The sub-system description does not imply the use of the centralized register (like in the previous case). E-documents (records) are issued in any form (photo, video, text and so on). These information resources can gain a status of a document in case of necessity, for instance, when being used as evidence in legal proceedings. As compared to the great amount of such information resources, while their proportion acquiring the document status is negligible.

Taking the foregoing into consideration, the ETR term was chosen as a general category, since it can describe (in the Methodology developers’ opinion) nearly the whole range of social functions inherent to the document per se. The issue of an electronic form of a document is the primary subject of the Methodology.

Thus, it seems possible to solve the problem of conversion of many documents into the electronic form reserving their social functions.

Since this issue is of the fundamental nature, it can be discussed in the framework of next events in the RCC format as well.