

**Methodology of the transboundary trust space (TTS)
forming and functioning in the Internet network**

Version 3.0

Moscow 2012

Contents

Introduction.....	4
Glossary	6
List of abbreviations.....	8
1 Analysis of the terms “a record” and “a document” in the context of fact-recording systems functioning.....	9
2 Description of the transboundary trust space architecture	12
2.1 Transboundary space architecture.....	12
2.1.1 Register systems	14
2.1.2 Common trust infrastructure	15
2.2 Interaction of the transboundary trust space elements	16
3 Description of a model process in the framework of the transboundary trust space	17
4 Peculiarities of paper documents conversion into an electronic form.....	19
5 Services of the common trust infrastructure.....	22
5.1 Signature service	25
5.2 Time service	28
5.3 Notary service	28
5.4 Apostil service.....	29
5.5 Location service	31
5.6 Legal status monitoring service	31
5.7 Payment security service	32
5.8 Trusted data storage service.....	32
5.9 Information service.....	33
5.10 Access service and requirements for reliable identification.....	33
5.10.1 Identifiers	35
5.10.2 Means of access.....	37
5.10.3 Attributes for division of an access to records.....	37
5.10.4 Access events logging.....	38
5.10.5 Key tasks	38
6 Examples of the common infrastructure services implementation in different subject areas.....	40
6.1 Supervisory bodies register systems	40
6.2 Medical register systems.....	43
6.3 Educational register systems.....	46
6.4 Legal regulation register systems.....	48
6.5 Business register systems	50
Conclusion	55

Supplement 1. A form for common trust infrastructure services performances selection 57

Supplement 2. Application of common trust infrastructure services for endorsement assurance 60

Supplement 3. Comparative analysis of the UNCITRAL document A/CN.9/WG.IV/WP.115 and the TTS Model 64

Introduction

Nowadays state bodies, natural persons and legal entities of different states need to obtain high quality electronic services, including transboundary ones (business, telemedicine services, distance education services, legal acts register and others).

One basic problem of an international electronic interaction is that a complex of organizational, technological and legal issues concerning electronic documents' validity assurance is still unsolved.

A solution to this problem implies a consolidation of register systems (hereinafter referred to as "RS") functioning nowadays within the transboundary trust space (hereinafter referred to as "the TTS"). Herewith, an assurance of these systems' interoperability is a necessary condition for their consolidation.

Today there exist a lot of organizations operating in the field of information documentation. In case of transition to the TTS such an aggregate of information systems will lead to heterogeneity of documents formed. For this reason it is necessary to distinguish documentation functions from RS and to form a separate (common for all) infrastructure.

To build a correctly functioning system some assembly point, which could be oriented at, is needed. The TTS Model¹ is suggested as such an assembly point.

In the present Methodology, development approaches and principles of the TTS Model based system of the transboundary electronic interaction are described.

The Methodology reflects a thesis, that the TTS Model, approved antecedently, is a constructive description of a complex engineering-humanitarian system. Herewith, the triune construction consisting of RS, electronic transferable records and a common trust infrastructure is the basis of all the structures.

An RS is responsible for a management of electronic transferable records (hereinafter referred to as "ETR") – a primary information resource possessing up-to-date information and validity. Documents are issued on the ground of the ETR. Subject to a specificity of one or another subject area, the RS can provide both an off-line and an on-line access to the data. The RS functioning is performed in compliance with the requirements for information documentation in electronic form.

The requirements imposed on the register systems depend on both a register system class and a subject area the system functions in. In the TTS the RS functions are limited to record management. The RS are built on the ground of the

¹ Model of the CIS member states' transboundary trust space forming and functioning in the Internet network

common trust infrastructure. The requirements imposed on the RS influence the common trust infrastructure implementation.

The Methodology also considers an issue, which solution is a necessary condition for ensuring a full-fledged international electronic interaction. This issue concerns a resolving of conflict situations arising in the process of electronic commerce. It is evident that with such a commodity circulation volume taking place at modern electronic trading platforms a resolution of each conflict situation in an international arbitral tribunal does not seem to be possible. Therefore, a development of a real time (on-line) dispute resolution mechanism is important. An on-line dispute resolution (hereinafter referred to as the “ODR”) peculiarity is that this process lacks a direct contact between information interaction participants, which is traditional for an arbitral dispute resolution, when a passport or another ID is a primary identification mean. Herewith, there appears a problem of a reliable remote identification of information interaction participants (a plaintiff, a defendant, a neutral party, ODR platform operators and ODR services providers). It is a development of requirements for a reliable identification of participants in the process of information interaction that is one of the Methodology subject matters.

The TTS forming implies a presence of the electronic information documentation rules regulating information interaction participants actions. Herewith, all the elements of such a system are to function in compliance with the statutes and regulations specially worked out (or adapted), including, in a particular, international treaties, commercial customs, legal acts in the field of the international commercial arbitration and insurance of risks connected with the use of transboundary valid information transactions.

Glossary

Accounting record (record) is data in electronic form recording subject of law legal status or recording an event happened. An accounting record comprises an aggregate of fields containing electronic content and document attributes – a result of documentation service and access service work. Accounting record's validity is assured by an aggregate of its attributes.

An applicant is an information interaction participant applying for a service to be rendered.

Audit of the register system operators' activity and common infrastructure or this infrastructure's separate components (services) is a system, created in compliance with an international treaty or commercial custom, controlling how these operators fulfil the requirements for information documentation in electronic form and respective activity regulations.

An authorized person is a person entitled to act on behalf of a register system operator, a common trust infrastructure service operator or an applicant.

Domestic (national) common trust space is an aggregate of normative and organizational-technical conditions for trust establishment in electronic information interaction of government bodies, other public bodies, state extra-budgetary funds, municipal bodies, legal entities and natural persons.

A common trust infrastructure is an aggregate of informational, technological, organizational and legal measures, rules and decisions performed in order to provide valid information interaction in the framework of the transboundary trust space. The common trust infrastructure consists of documentation services, an access service and a number of secondary services.

A common trust infrastructure service operator is an organization entitled in compliance with national legislation of each member to an international treaty (an authorized operator) or in compliance with commercial custom (a trusted operator) to carry performance of legal functions on the ground of the common trust infrastructure or individual components (services) of this common trust infrastructure.

Common transboundary trust space is an aggregate of normative and organizational-technical conditions for trust establishment in transboundary electronic informational interaction of state government bodies, other public bodies, state extra-budgetary funds, municipal bodies, legal entities and citizens.

Trust is a ground for an assurance that an essence serves its security purposes.

Electronic information documentation requirements are a set aggregate of informational, technological, organizational and legal measures, rules and

decisions in a part of the common infrastructure - based register systems construction, particularly, object identifiers utilization.

Electronic information documentation rules are set regulations of activity performed by the common infrastructure - based register system participants' - information interaction subjects, including authorized persons of register systems and common infrastructure components (services) operators and users.

An electronic transferable record is a type of accounting records designed to assign legal relations subject's rights, created by a register system and comprising an aggregate of fields containing electronic content and document attributes – a result of the common trust infrastructure services work.

A fact-recording system is a system designed to register legal facts.

A major fact-recording system is an agreed aggregate of electronic fact-recording systems.

An operator's auditor is an organization entitled in compliance with national legislation of each member to an international treaty (an authorized operator) or in compliance with a commercial custom (a trusted operator) to audit:

- activities of register system operators;
- activities of common infrastructure operators;
- Activities of operators of the infrastructure individual components (services).

An auditor operates in compliance with regulations approved.

A procedure is a formalized, regulated process phase.

A process is a sequential transition of states, development stages of an event considered and a certain aggregate of sequential actions aimed at some objective to be achieved.

A register system is a registration information system containing an aggregate of accounting records (primary register records stored), combined in storages and administered by input, storage and conversion mechanisms, containing information from the information interaction participants' documents of title, with valid electronic transferable records being drawn up or issued on the above grounds.

A register system operator is an organization entitled in compliance with national legislation, legislation of each member to an international treaty (an authorized operator) or in compliance with a commercial custom (a trusted operator) to carry out administration of the electronic resources containing an aggregate of information interaction subjects' documents of title.

Transboundary information interaction is an information interaction of different legal frameworks' subjects.

List of abbreviations

ES – an electronic signature

ETR – an electronic transferable record

FRS – a fact-recording system

IIP – an information interaction participant

MFRS – a major fact-recording system

NTS – a national trust space

ODR – an on-line dispute resolution

RS – a register system

TTS – a transboundary trust space

1 Analysis of the terms “a record” and “a document” in the context of fact-recording systems functioning

Specialists in the field of electronic document flows are well aware of differences between the terms “a record” and “a document”, stated in international and domestic standards (ISO 15489 and its derivatives in different states).

These differences result from two different approaches to fact-recording systems’ (FRS) functioning description: an integral and a differential approach.

The integral approach combines the terms “a record” and “a document” in a single term “a document” and is characterized by the presence of a significant transport component. Such an approach can be demonstrated through the following practical examples: the paper document flow, electronic records management and e-mail, including the protected one (the interdepartmental electronic records management). In these systems some units, generally called “documents” are delivered and registered, that completely corresponds to these systems functions. But alongside with the electronic contour of the information exchange there is another contour – the paper one. Thus, the interoperability between the two system parts is reached.

A documentation process, characteristic for both paper and electronic systems, consists of the following procedures (fig. 1):

- A recordkeeping procedure – information recording;
- A documentation procedure² - document issue on the ground of a record.



Fig. 1. Information documentation

Fact-recording systems’ functions in electronic form (the e-FRS) consist in organization of separate access to the records organized in a special way in the registers, records, cadastres and fixed in data bases. This is an information-security technology, not a telecommunication one. In case of such systems description, it is reasonable to use the differential approach, which allows to transmit from an amount of paper (“physical”) documents to an organized aggregate of the electronic transferable records (hereinafter referred to as “records”) in electronic data bases.

² Documentation is a recording of information on different media according to the rules set – GOST R 51141-98.

In the context of an e-FRS functioning, a record is the key element of this system's interaction. A record is generated and stored in centralized data bases and it is valid.

Documents are valid as well, but are issued on the ground of records. In this case a record is some standard, it is on-line current. Documents, being on hand of information system users, actually have an off-line status, since from their issue date a certain period of time inevitably elapses. During this period some right can be altered or terminated. Thus, a record is the primary e-FRS element and a document is a secondary one.

Systematized records in a data base are the FRS core, while documents are peripherals. The core's operators are authorized bodies (persons) whose activity is regulated and audited. The core is formed on the functional ground, for instance, the records in respect of legal entities or real estate registration. Service (obtainment of documents) applicants are the peripherals' operators. Such operators are to assure integrity of a document obtained in result of a service provided and its valid use (filing). An aggregate of such documents can be located at the applicant's place (for instance on a flash-device) or in his personal profile, accessible through the Internet.

Basic differences between the terms "a record" and "a document" are displayed in Table 1.

Table 1

The terms "a record" and "a document" differences

Record	Document
Primary information resource	Secondary information resource (issued on the ground of the record)
Data status: on-line	Data status: off-line
Records refer to the FRS core	Documents refer to the FRS peripherals

It should be also remarked, that one of the e-MFRS principal differences from paper major fact-recording systems (p-MFRS) is as follows (Table 2). In p-MFRS recording procedures and information documentation in paper form are carried out in the framework of a single authorized body. In the framework of e-MFRS the information documentation function is taken away from the bodies authorized to administer the register systems. Herewith, an electronic information documentation infrastructure appears. It can consist of different services.

Table 2

Differences between paper and electronic major fact-recording systems

p-MFRS		e-MFRS	
↓ Recordkeeping procedures	↓ Procedures of information documentation in paper form	↓ Register system	↓ Infrastructure information documentation in electronic form
		↓ Recordkeeping procedures	↓ Procedures of information documentation in electronic form

The e-MFRS architecture is described below.

2 Description of the transboundary trust space architecture

2.1 Transboundary space architecture

The transboundary trust space (the TTS) is an electronic major fact-recording system functioning on the transboundary level (the MFRS-T). The TTS comprises major fact-recording systems of the national level (the MFRS-N).

Each MFRS-N consists of a number of register systems and services of the common trust infrastructure which is common for the whole MFRS-T.

Each register system and common trust infrastructure service has its own operator. The operators' authorized persons are to interact with the applicants in order to facilitate services obtainment.

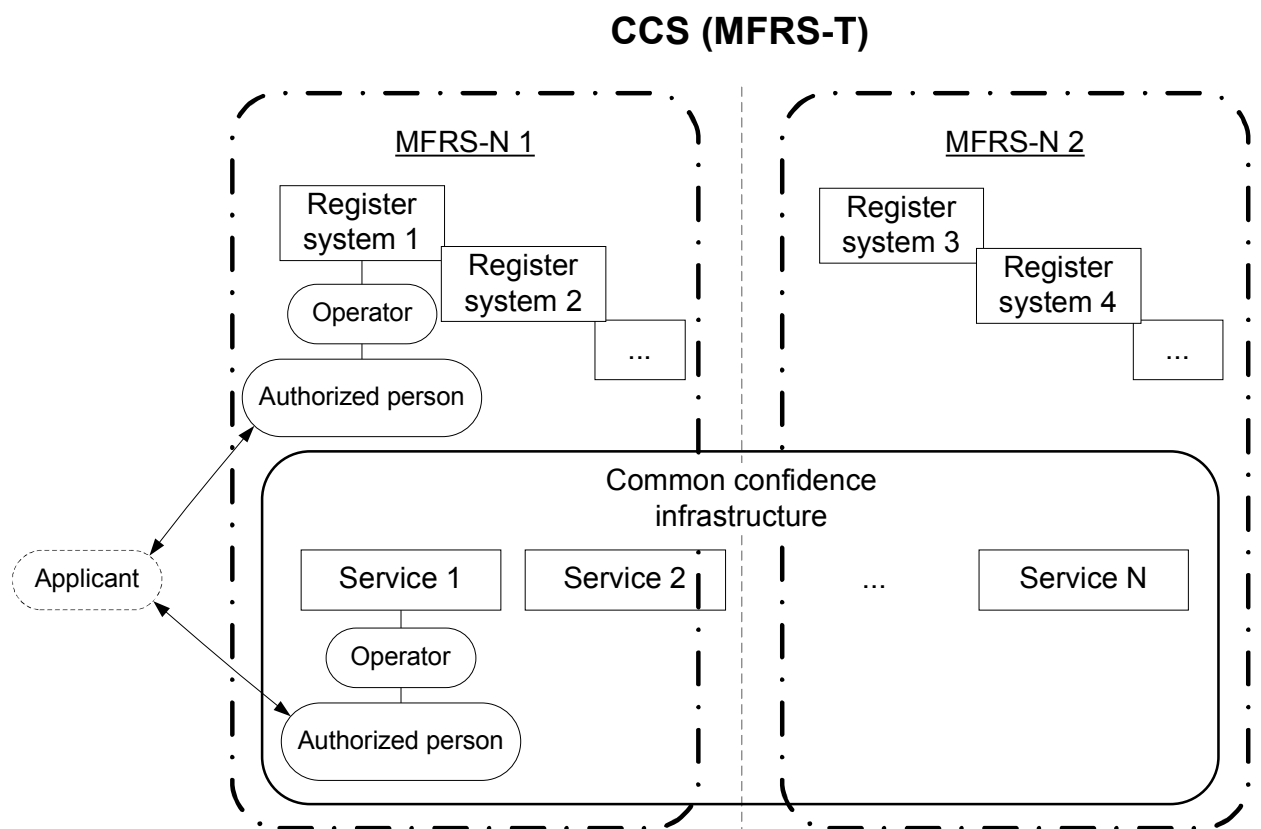


Fig. 2. The TTS architecture.

The TTS is an integrated complex consisting of institutional, legal, organizational, statutory, technical, technological units capable to assure a correct functioning of the whole system and its individual elements.

Therefore, when forming the TTS, it is necessary to take into account inter-linkages between the elements of the TTS and its units (Table 3).

Table 3

The inter-linkages of the TTS elements and units

The TTS elements	The TTS units		
	Institutional and legal	Organizational and statutory	Technical and technological
Register systems	Regulatory documentation		Information documentation requirements
Common trust infrastructure	Regulatory documentation		Information documentation requirements
Register systems' operators	Regulatory documentation	Activity regulations	Information documentation requirements
		Activity audit	
Trust infrastructure services' operators	Regulatory documentation	Activity regulations	Information documentation requirements
		Activity audit	
Operators' auditors	Regulatory documentation	Activity regulations	
Authorized persons	Regulatory documentation		Information documentation rules
Applicants	Regulatory documentation		Information documentation rules

2.1.1 Register systems

In contrast to systems of electronic document management (EDMS) and interdepartmental document flow (IDFS), register systems operate with records antecedent to the forming of new documents of title forming. In this connection the register systems are more critical in the context of information stored (operated) in comparison with EDMS and IDFS. Therefore, tougher requirements, in their turn depending on register systems' class and type, can be imposed on them.

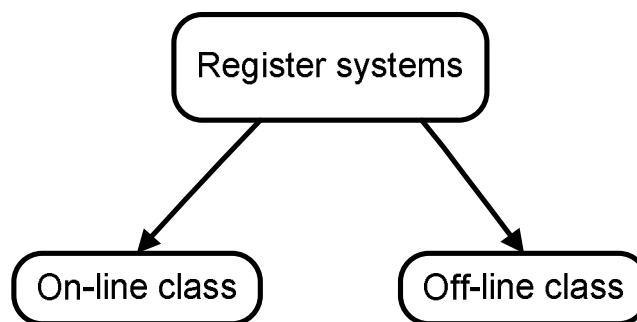


Fig. 3. Register systems classes

Subject to the content access method, register systems can be subdivided into the two classes (fig.3): on-line and off-line.

On-line class RS imply that a user can verify a document's authenticity in real time mode via applying to a respective service of the common trust infrastructure. Herewith, such a verifying system is of regular character.

On-line class RS are designed to fix legal states of subjects of law (natural persons and legal entities) and to enable supervisory bodies' officers to apply periodically to the system core and a centralized data base for verification of a claim an applicant presents.

Such RS are run in respect of individual characteristics of subjects and objects of law (citizenship, licenses, certificates, accreditations, cadastral register and many other rights).

Off-line class RS are designed to assure legal relations. Valid information in the form of records is accumulated gradually (for instance, in the framework of a patient's history, periodic exam pass, contractual obligations performance etc). An external on-line access to these records is not needed, but is often detrimental for privacy or commercial secrets. Off-line class RS are run in respect of subjects and objects of law.

A subject area, where a certain RS work, is connected with influences by requirements imposed on RS building and functioning as well.

Examples of subject areas where RS can be applied:

- Supervisory bodies register systems;
- Medical register systems;
- Educational register systems;
- Business register systems;
- Legal regulation register systems;
- Others

Any RS included in the TTS implies an operator of this RS, administering electronic registers, containing an aggregate of information interaction subjects' documents of title.

The RS operators are to work in compliance with the regulations adopted.

RS operators' work is to be audited.

The following statuses of RS operators are suggested:

- a state organization;
- a commercial organization.

RS are based on the common trust infrastructure. Herewith, the requirements imposed on RS influence the common trust infrastructure implementation.

2.1.2 Common trust infrastructure

The common trust infrastructure (hereinafter referred to as “the common infrastructure”) consists of a number of services - providing on the information technology basis - legal processes and states formalization.

The common infrastructure can be created on a single-domain or a multi-domain basis depending on the number of legal areas, information interaction participants relate to. In case the multi-domain scheme is used, all the domains are to be harmonized. It is provided via applying common electronic information documentation rules and requirements.

The present Methodology suggests to use the multi-domain trust principle, whereby each domain is a national trust space (NTS). In order to provide interoperability of domestic electronic document flow contours, the NTS is to be created as an interacting TTS subsystem.

The common infrastructure services can be divided into three categories:

- Documentation services;
- Access services;
- Additional services.

A list of the necessary services is subject to the requirements for the common trust infrastructure - based register systems and to the requirements for the NCS in whole.

Each service implies an operator working in compliance with regulations approved, with their activity being audited.

2.2 Interaction of the transboundary trust space elements

Interaction between register systems and between an applicant and a register system can be divided subject to the legal areas (jurisdictions) participants relate to. Therefore, 3 types of information interaction can be singled out:

- Mono-jurisdiction (the participants are under jurisdiction of one state);
- Multi-jurisdiction (the participants are under jurisdiction of different states);
- Quasi-mono-jurisdiction (the participants are under jurisdiction of different states, with the integral information space formed).

3 Description of a model process in the framework of the transboundary trust space

Register and information process underlies functioning of any MFRS. Like any other process, it consists of a start phase, an aggregate of intermediate phases and an ending phase. Each phase is characterized by a certain level of alterations in the system. Relations of the alterations level to a process phase can be demonstrated (Fig.4).

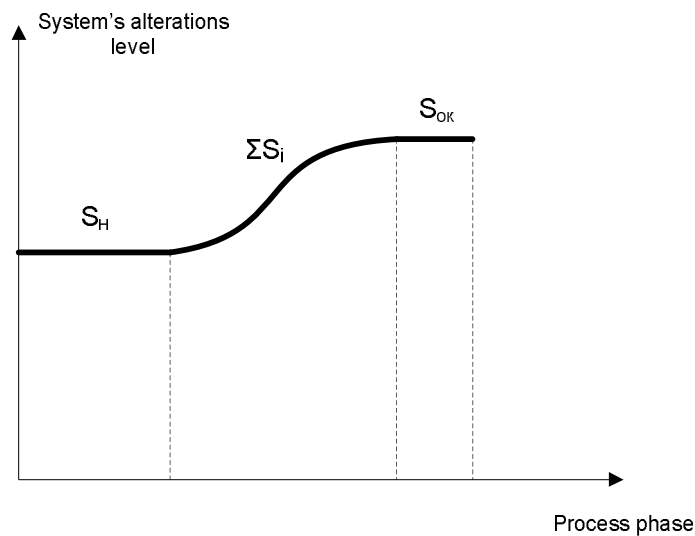


Fig. 4. Diagram of alterations in a system

We can see at the diagram, that in the start phase (S_s) the system is stable – there are no alterations in it. Then the intermediate phases come (ΣS_i), characterized by some alterations in the system. After the alterations are finished, the system is “leveled up” and stable again – this is the ending phase (S_e). This diagram can be specified with regard to the TTS.

At the phase P_1 (fig. 5) the system is originally stable. Then alterations are activated in the system, but the system itself is still stable – phase P_2 . The phase of the first alterations in the system (P_3) can be described as a synthesis of the regulated information aggregate in the form of certificates or documents to be filed to an authorized body in the system. Then there comes adaptation of a demand formalized to existing laws, legal acts, regulations (P_4) and a result is recorded in a respective register system (P_5). After that, the system changes over to the new stable condition – the phase of regulated records storage in a data base (P_6).

Thus, for the TTS we can point out a model register and information process, characteristic for any type of register systems, information interaction, and

irrespective of the subject area under consideration. This process consists of the following phases:

- a phase of a stable system (P_1);
- a phase of a system alterations activation (P_2);
- a phase of a synthesis of a regulated information aggregate in the form of certificates or documents to be filed to an authorized body (P_3);
- a phase of adaptation of a demand formalized to existing laws, legal acts and regulations (P_4);
- a phase of result recording in the respective register system (P_5);
- a phase of regulated records storage in a data base, organization of a separate access to them (P_6).

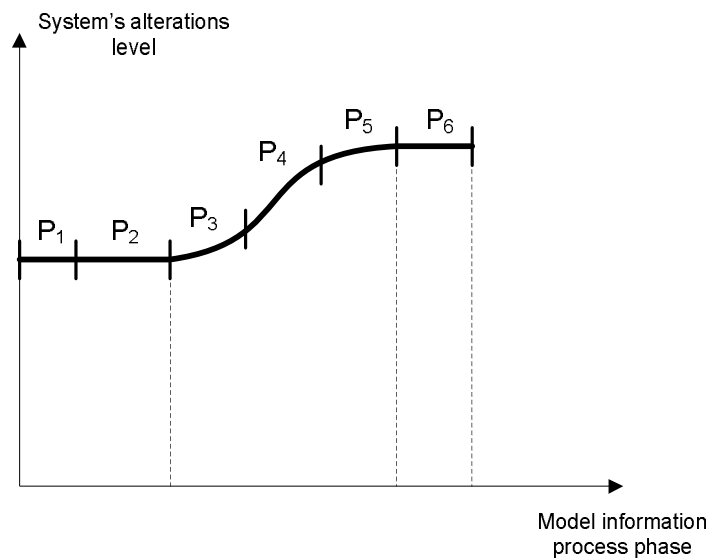


Fig. 5. A diagram of system alterations in a model information process.

Characteristic peculiarities of a register and information process depending on the subject area under consideration will be demonstrated further.

4 Peculiarities of paper documents conversion into an electronic form

Paper document validity is provided by an aggregate of its attributes, with the urgency of the contained information being its important peculiarity.

One of the primary requirements for paper documents conversion into an electronic form is to reserve integrity and systemization of document's attributes. It is stipulated by the fact that the attributes aggregated perform document validity. Loss of an attribute (for instance, a date) can make a document null and void.

Information interaction in a part of working with e-documents demands e-document attributes confirming its content and assuring validity as well.

Reservation of e-documents attributes' properties in the e-MFRS (for example, in the TTS) can be assured via using documentation services.

One could mention a signature service, a time service, a notary service, an apostil service, a location service and a legal status monitoring service as examples of documentation services.

Besides reservation of the e-documents attributes' properties, it is necessary to organize a separate access to these documents. It is reached via using the access service.

Also in some cases additional (optional) services, which are not necessary but capable of providing a wider range of qualitative services, are demanded. For instance, there are services, like a payment security service, a trusted data storage service and an information service.

Each of the common infrastructure services can be performed in different ways. A selection of a particular performance depends on a level of trust between information interaction participants.

At a high level of trust the Light-requirements are imposed on the service's performance. The existing systems of an electronic document management and interdepartmental electronic document flow can be taken as an example of the systems fully constructed in compliance with the Light-requirements.

The services' performance according to the Medium- or Heavy-requirements means service centralization or decentralization respectively. The middle level of trust enables to construct a service on the centralized basis (Table 3), while the low level of trust requires decentralized performance.

Table 3

Correlation of a trust level between the information interaction participants and the service performance requirements

Level of trust between the information interaction parties	Service performance requirements
High	Light- requirements <i>(without application of trust services, in some cases existing performance)</i>
Middle	Medium- requirements <i>(centralization)</i>
Low	Heavy- requirements <i>(decentralization)</i>

It should be mentioned, that the present division is relative and for each particular service a number of its optional performances can differ from three.

There exist many options of the services combinations and their performances depending on register and information process peculiarities. But generally, system performance cost dependence on the security level and services quality selected will be monotonically increasing (a trend line in the Figure 6). According to the necessary information interaction level of security and services provided quality (B_1) a certain set of services (as well as their performances) is to be selected. At the same time, there appear respective costs of constructing and operating such system (C_1).

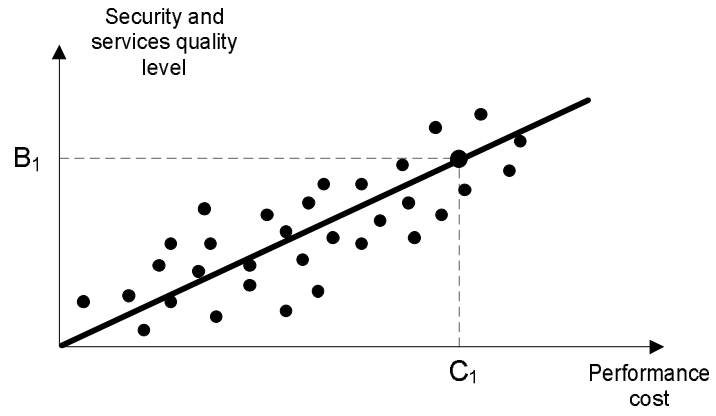


Fig. 6. Diagram of a system performance cost dependence on the security and services quality level selected.

5 Services of the common trust infrastructure

This section presents the first approximation of common trust infrastructure services. These services are primarily designed to assure interactivity³ of documents details (attributes). Herewith, special attention is paid to legal content of these attributes.

At present in the Russian Federation a list of such attributes is set⁴. This list is not a random set of the document characteristics but an integral system of data, inextricably connected to a document. This system is designed to assign validity to informational content of an official document issued by authority bodies in course of duty both in interdepartmental interaction and in interaction with other subjects of information interaction, with citizens and organizations first of all.

This property of attributes' integrity and systematization is to be reserved when forming a list of the common infrastructure services, because in the aggregate they will perform an integrated validity property of information interaction between subjects – natural persons and legal entities.

Table 4 shows these attributes grouped on the basis of necessity and possibility to converse an attributes system into an electronic form on the ground of state-of-art information (first of all, information security) technologies.

³ Interactivity means an ability to be altered and verified in the on-line mode

⁴ Art. 10 Rules of records management in federal executive bodies, approved by the Government of the Russian Federation Decree dated June 15, 2009 № 477.

Table 4

A grouping of documents attributes on the basis of necessity and possibility to perform their interactivity⁵

№	Grouping criteria	Name of document attributes	Comment on attributes conversion into the electronic form
I.	Content	1) document body 2) document type 3) document title 4) mark about supplements (<i>hyperlink</i>)	An aggregate of these attributes is the content, the informational essence of a document, which is to be irrespective to an expression form – whether paper or electronic one. Herewith, information integrity, credibility and authenticity are to be assured when processing, storing and transferring. In electronic form: Integrity is assured through using of an electronic signature. Credibility can be ascertained only through comparing of a document's content and reality facts to the moment a document's content is formed, and through electronic signature verification. Authenticity is ascertained only through using of an electronic signature.
II.	Authority legal status	5) state emblem 6) name of a federal executive body 7) federal executive body reference data 8) seal impression	Is to be performed trough forming of a federal executive body electronic register as an infrastructure component assuring the validity property (hereinafter referred to as “the validity aspect”) as a properly formalized, recorded legal fact. Such an approach can be suggested for other regional and municipal authorized bodies.
III.	Authorized persons legal status	9) post of the person signed (<i>approved, negotiated, backed, legalized a copy</i>) a document	Is to be performed trough forming of an electronic register of authorized persons, containing a brief description of powers with their duration stated.
IV.	Signature	10) officer's signature 11) conformation visa 12) approval visa 13) visa 14) copy legalization mark	Is to be performed trough using of an electronic signature which legal content is an expression of will of a signature key certificate holder registered in the CA register (the validity aspect). <i>Note:</i> This holder's official status is to be additionally proved via applying to an electronic register of authorized persons or can be fixed with a special attribute in his signature key certificate. The will expression form (signature, negotiation, approval, visa, copy legalization) can be stated in a document body, included to an electronic signature or reflected in metadata to a record in an electronic data base.
V.	Document management	15) document register number 16) reference to an outgoing number and date of a sender's document	These attributes are accessory to a final document and are not independent aspects of the integral validity property. They are being on the basis of departmental electronic systems of document management, which are not

⁵ The list of attributes is extracted from the Government of the Russian Federation Decree dated June 15, 2009 № 477.

		17) execution mark 18) instructions for document execution 19) document control mark 20) document execution mark 21) confidentiality mark	reasonable to be referred to a common electronic document flow infrastructure assuring the integral validity property above.
VI.	Place	22) document's place of issue	Electronic attestation with specially authorized or trusted persons involved (the validity aspect). It is characteristic for transactions, contracts, treaties, agreements being concluded between two or more parties located in different geographic places and probably under different jurisdictions
VII.	Time	23) document's date	Time stamps, attached on the basis of a trusted time source (the validity aspect).
VIII.	Other information interaction subjects	24) addressee (<i>applicant</i>)	Electronic registers of natural persons and legal entities (the validity aspect).

The attributes which, in compliance with existing standards, resolutions and other legal acts regulating a document flow, are to be present in a paper document, according to the Table given, shall be reserved when conversing to an electronic form. Herewith, attributes authentication confirmation is proposed to be ensured by using the common trust infrastructure services, including documentation services, additional services and an access service.

The documentation services are:

- A signature service;
- A time service;
- A notary service;
- An apostil service;
- A place service;
- A legal status monitoring service;

The additional services are:

- A payment security service;
- A trusted data storage service;
- An information service.

The service set given cannot be regarded as complete and can be complemented if necessary.

Each service can have several options of performance, whereas their description approach can be based on the concepts of centralization/decentralization and mono/multi-jurisdiction. In other words, it is suggested to consider three available performances of each service.

Light-performance implies service's function execution by a register system itself for the majority of the services.

This services performance reflects the current paradigm of an e-document – a document, which attributes are static. Register systems’ interoperability is generally assured using paper copies of documents.

The Light-performance is added to the services descriptions to reserve the structure and demonstrativeness of this Methodology.

Medium-performance implies that a service is organized centrally for several jurisdictions. A single service operator serves subjects of different jurisdictions.

Heavy-performance implies that a service is organized in a decentralized way for several jurisdictions. In each jurisdiction there is one or several operators serving subjects of the same jurisdiction. Operators of different jurisdictions interact with each other.

A selection of a centralized or decentralized option depends on a level of trust between register systems’ operators of different jurisdictions. At a *high* level of trust some common infrastructure services can be performed centrally, being administered by a single international operator. At a *low* level of trust all the common infrastructure services are performed in a decentralized way – in each jurisdiction there is, at least, one “domestic” operator. The transboundary aspect is enabled via interaction between such domestic operators.

In the services performance descriptions below references to technical solutions, which the Methodology drafters consider to be the most compliant with the requirements indicated in the register systems of different subject areas, are given. Technical solutions, not stated in this Methodology, can also be acceptable if harmonized with the TTS Model architecture.

Special attention should be drawn to the point that the common trust infrastructure will be constructed on the basis of *certain technical solutions*. There will be a final number of interfaces unified. Through them register systems will be able to interact and to apply to the common infrastructure services. Thus, any register system’s operator will have to put the RS interfaces in compliance with the common infrastructure interfaces in order to provide RS interoperability.

5.1 Signature service

A signature service is designed to confirm a will expression of natural persons – information interaction participants. The following service performances are suggested.

Light-performance – an expression of a participant’s will is confirmed in the process of an interactive dialog in an RS interface (an RS itself). In a system’s data base a label is set indicating that a particular user acted one way or another or agreed with this or that provision. Decisions providing functions of a corporative

electronic signature also relates to this implementation. The corporative electronic signature means an electronic signature which is valid only within a single organization or a particular final group of organizations. In this case electronic signature utilization is regulated by by-laws or agreements concluded by organizations.

Medium-1-performance – an expression of a participant’s will is confirmed by his/its electronic signature. A participant’s (signatory’s) electronic signature certificate⁶ is issued by a certification authority. This certification authority has an international organization status and representatives in each jurisdiction. In this case a CA is a signature service’s centralized operator.

A mathematical verification of an electronic signature (a verification of signed data integrity) is carried out locally in a CA. A signatory’s certification status verification is carried out through RS accessing to the CA⁷.

Advantages and disadvantages of this performance are evident. The former are simplicity of technical implementation, administration and audit. The disadvantages are higher requirements for service security, continuity and performance.

Note 1. In this and below-described signature service performances an advanced electronic signature technology⁸ can be applicable. Its difference is that an electronic signature format contains information about status of the signatory’s certificate *at the moment the electronic signature issuance*. The moment an ES issued is assured with the time service⁹ operator’s ES (a time stamp is attached to the ES). A certificate status is verified via RS accessing to an on-line certificates status verification service of a CA issued the signatory’s certificate. A response (receipt) of a CA on-line certificates status verification service is signed with this service operator’s ES. An advanced ES formed this way guarantees a validity of a signatory’s certificate *at the moment the ES formed* in contrast to a “simple” ES, whereby a certificate’s validity can be defined only for *the moment the ES is verified*. A time stamp can be used as an evidence of data possession (the data signed with an advanced ES).

Note 2. In this and below-described signature service’s performances descriptions a technology of a participant’s electronic signature *validation* with an electronic signature of another participant (for instance, validation with a notary’s electronic signature) is available.

⁶ see. ITU-T X.509

⁷ Hereinafter, “an access to a CA” means an access to a certificate revocation list (CDP - RFC5280) or to an on-line service of certificate status verification (OCSP - RFC2560).

⁸ see. RFC5126

⁹ The TSP protocol (RFC3161) can be an example of the implementation.

Medium-2-performance - an expression of a participant's will is confirmed by his/its electronic signature. A participant's (signatory's) electronic signature certificate is issued by a CA functioning in the same jurisdiction the participant functions in (a national CA). This national CA has trust relations with analogous national CA of other jurisdictions. At that, the national CA is a part of a certification authorities hierarchy headed by a CA having an international organization status.

Each national CA can have several subordinate CA. In other words, within the limits of one jurisdiction there exists a hierarchal structure of certification authorities, headed by a single national CA having trust relations with analogous national CA of other jurisdictions.

Heavy-1-performance – an expression of a participant's will is confirmed by his/its electronic signature. A participant's (signatory's) ES certificate is issued by a CA functioning in the same jurisdiction the participant operates in (a national CA). This national CA has trust relations with analogous national CA of other jurisdictions. Herewith, the trust relations can be built on the principle of cross-certification of national CA.

Each national CA can have several subordinate CA. In other words, within the limits of one jurisdiction there exists a hierarchal structure of certification authorities, headed by a single national CA having trust relations with analogous national CA of other jurisdictions.

Unlike the **Medium-1-performance** the **Medium-2** and **Heavy-1-performances** imply an allocation of burden among CA (each CA serves subjects of its jurisdiction) and higher fall-over protection of the service in whole. Another advantage of these performances is a capability to build a certification authorities structure based on *existing* operators – private and public certification authorities.

At the same time the key moment to be noted is that the present **Medium-2** and **Heavy-1-performances** imply that each information interaction subject has electronic signature means performing all the cryptographic algorithms applied in this PKI architecture.

Heavy-2-performance - an expression of a participant's will is confirmed by his/its electronic signature validated with an apostil service operator's ES (available apostil service performances are described below). The RS and CA issued a signatory's ES can be subjects of different jurisdictions (subjects of different states).

The ES verification order is as follows. An RS forwards a request for a signatory's ES verification to an apostil service. A mathematical verification of the ES (signed data integrity verification) is carried out locally by the apostil service.

A signatory's certificate status verification is carried out via the apostil service accessing to the CA issued the signatory's certificate. A receipt, containing results of the party's ES mathematical verification, signed with the apostil service operator's ES results of the party's certificate status verification and verification time¹⁰, is forwarded to the RS. This receipt is stored in the RS and can be prolonged via accessing to the apostil service, that enables to provide verification of the party's ES upon the expiration of his/her certificate.

5.2 Time service

The time service is designed to confirm the operation's performance time, for instance, the alteration time of a profile, with an on-line separate access to it being organized, or time of an off-line document's issue on the ground of this profile. The following service's performances are available:

Light-performance – local RS clock time is stated as an operation's performance time. The local RS clock is synchronized with some public network time server¹¹.

Medium-performance – local RS clock time is stated as an operation's performance time. The local RS clock is synchronized with the common infrastructure time service and an operation's performance time can be certified with a time service operator's ES if demanded. The time service's local clock is synchronized with standard time signals¹².

Heavy-performance – operation's performance time is certified with a time service operator's ES¹³. Time service local clock is synchronized with standard time signals.

5.3 Notary service

The notary service is designed for an unconditional validation of a natural person's will, performed with application of an electronic signature data. Performance of notary actions and/or actions with electronic documents with application of a notary's ES is a notary service's function.

Notary service's functions are as follows:

¹⁰ Structure of receipts issued by the apostil service and notary service can be harmonized taking into account RS needs.

¹¹ For instance, synchronization of RS clock through the NTP-protocol with the Microsoft ntp-servers, VNIIFTRI NTFS (national time and frequency standard) etc.

¹² Synchronization can be performed via the satellite constellation GLONASS/GPS signals or via atomic time standards signals.

¹³ The TSP-protocol (RFC3161) can be taken as an example.

- a conversion of documents drawn up on a paper medium into an electronic form without losing their validity, inherent to a paper document by virtue of its attributes;
- a conversion of documents drawn up on a paper medium into an electronic form without losing of its validity, inherent to an electronic document by virtue of its electronic signature;
- an unconditional validation of a natural person's will performed in the notary's presence by means of a participant's (will expresser's) electronic signature¹⁴ validation with a notary's electronic signature;
- a notary validation of transactions in electronic form by placing of an extra electronic signature¹⁵ (a notary's ES) on the data recording the transaction.

The functions set given cannot purport to be complete and can be complemented if necessary.

The notary service's peculiarity is that notary participation as a subject in the process of the functions stated is necessary. It means that a concept of a centralized operator is inapplicable to a notary service. Therefore, the service's **Heavy-performance** with a decentralized operator (implying a notary or notarial system) is the only one to be considered.

Trust between notary institutions of different jurisdictions can be assured via an apostil service.

5.4 Apostil service

An apostil service is designed to validate data (content, a signature, content encrypted etc) for valid application within different jurisdictions. In other words, an applicant (an RS or another information interaction subject) and the CA, that issued a signatory's ES certificate to be verified, belong to different jurisdictions.

The apostil service issues the following types of receipts¹⁶ on demand of an RS and other information interaction participants:

- A ES verification results receipt;
- A signatory's certificate validity verification receipt.

Receipts issued by the apostil service can be extended through a respective enquiry.

¹⁴ The concept of "an electronic signature validation" correlates with the concept of "signing by a counter signature" used in the UN/CEFACT Recommendation 37.

¹⁵ The concept of "an extra electronic signature" correlates with the concept of "a co-signature" used in the UN/CEFACT Recommendation 37

¹⁶ cm. ITU-T X.842

Medium-1-performance – this performance implies a centralized architecture. In this architecture there exists a single apostil service interacting with all the CA, with the latter functioning in different jurisdictions.

ES verification includes signed data integrity verification and signatory's certificate status verification. The signed data integrity verification is carried out by an apostil service locally. The signatory's certificate status verification is carried out by apostil service's reference to the CA issued the signatory's certificate. A receipt, signed by an apostil service operator's ES and containing ES verification results, is forwarded to the applicant.

This performance simplifies procedures of apostil service's activity administration and audit. Higher requirements for service reliability, continuity and performance are the disadvantages. Moreover, an apostil service is to have technical resources to work with all the cryptographic algorithms applied by the CA it interacts with.

Medium-2-performance – this performance implies a centralized architecture. In this architecture there exist national apostil services in each jurisdiction interacting with each other through a "bridge" apostil service possessing an international organization status.

In this case the work order is as follows. An applicant forwards an enquiry for ES verification to a national apostil service (belonging to the same jurisdiction as the applicant). The national apostil service redirects the enquiry to a bridge apostil service which, in its turn, redirects the enquiry to the national apostil service interacting with the CA, which issued a signatory's certificate. An ES verification receipt is redirected to the applicant the same way in a reverse order. In this performance an applicant interacts directly with an apostil service of his/its jurisdiction only; procedures of bridge apostil service and national apostil services interaction are concealed for the applicant.

This performance lacks one of the apostil service **Medium-1-performance** disadvantages, namely, a necessity for a bridge apostil service to have technical resources to work with all the cryptographic algorithms applied by CA, which certificates are verified. At the same time higher requirements for bridge service's reliability, continuity and performance remain.

Heavy-performance – this performance implies a decentralized architecture. In this architecture national apostil services of different jurisdictions interact directly.

In this case the work order is as follows. An applicant forwards an enquiry for ES verification to a national apostil service (belonging to the same jurisdiction as the applicant). The national apostil service redirects the enquiry to the national

apostil service interacting with the CA, which issued a signatory's certificate. An ES verification receipt is redirected to the applicant the same way in reverse order. In this performance an applicant interacts directly with a national apostil service of his/its jurisdiction only; procedures of national apostil services' interaction among themselves are concealed for the applicant.

Interaction among notary services is carried out using specialized certificates. Specialized certificates' data life cycle management is carried out by a single CA; this CA operator has an international organization status.

On the one hand, such an approach provides an opportunity of notary services infrastructure centralized administration, but, on the other hand, provides a burden allocation among national apostil services and increases infrastructure reliability in whole. However, there appears a necessity to set forth a unified cryptographic algorithm, used in the process of national apostil services' interaction.

5.5 Location service

A location service is designed to certify the place an operation performance place (for instance, a place a record is made or an e-document is issued in).

Light-performance – an RS record contains an attribute stating a document's issue place. An attribute's value is filled in by a register system itself.

Medium-performance – an operation's performance place is certified with a notary's electronic signature.

Heavy-performance – an RS record contains an attribute stating coordinates of operation's performance place¹⁷. The coordinates are certified by a location service operator's ES.

5.6 Legal status monitoring service

An information interaction subjects' legal status monitoring service (hereinafter referred to as “the LSMS”) is designed to register, maintain current and terminate legal status of information interaction subjects – legal entities, as well as natural persons' competence, powers and signatory authorities.

Light-performance – subject's legal status management is carried out by an operator of an RS itself.

Medium-performance – subject's legal status is stated in his/its ES certificate. Subject's status primary verification is carried out by the CA issuing the certificate.

Heavy-performance – subject's legal status is stated in his/its attributive certificate¹⁸. An attributive certificate can be connected in a unique manner with a

¹⁷ For instance, coordinates received from satellite constellations GLONASS/GPS.

subject's certificate or any other document. Attributive certificate's life cycle management is carried out by an LSMS operator, which work algorithm is analogous to the work algorithm of the CA managing ES certificates' life cycle.

The service has a decentralized architecture and, as well as signature service's performances, trust relations between different LSMS operators can be built:

- a) On the principle of cross-certification or LSMS hierarchy headed by a LSMS having an international organization status – LSMS service's **Heavy-1-performance**;
- b) Using an apostil service – LSMS service's **Heavy-2-performance**.

The advantage of this performance is that there is no necessity to re-issue an ES certificate at subject's powers alteration. A subject's certificate is issued for a long period of time and is re-issued only in case of subject's identification data alteration (for instance, his/her last or first name, patronymic). At the same time an attributive certificate reflects subject's powers and can be re-issued any time when subject's powers are altered (for example, in case of subject's position alteration). A subject can have an unlimited number of attributive certificates, with each being responsible for one or another type of powers.

5.7 Payment security service

A payment security service is designed to confirm payment of fees, tariffs, taxes etc, connected with legally significant actions commission.

Light-performance – a subject pays for services of each RS he/it interacts with. At that, mutual settlements are performed directly with an RS operator.

Heavy-performance – a subject pays for a services complex, which includes availability to use a set register systems and common infrastructure services aggregate. Herewith, a cost of the services complex named can be built into the cost of subject's ES certificate issue and life cycle support.

5.8 Trusted data storage service

A trusted data storage service is designed to perform some «safe-deposit box» in which one can store legally significant information, in an encrypted form as well, in respect of individual natural persons and legal entities (under contract) in case when such data storage for one's own account appears to be excessively expensive or insecure for a user.

Light-performance – data is stored locally in each RS.

Medium-performance – data is stored locally in each RS. Data access is carried out with application of an LSMS.

Heavy-performance – data is stored in a trusted storage service in an encrypted form with application of asymmetric encryption¹⁹. Data access is performed using the LSMS. Data transmission to a storage service is carried out via a secure path.

5.9 Information service

An information service carries out reference and informational function – it enables users to get acquainted with various RS data.

Light-performance – an information service contains static materials²⁰. A service is performed by register system's means.

Medium-performance – an information service contains dynamically changing materials²¹. The service is carried out by register system means.

Heavy-performance – the information service contains dynamically changing materials²². A service is performed by an individual operator (operators), guaranteeing higher requirements for an information accessibility.

5.10 Access service and requirements for reliable identification

A performance of information transactions online implies that there is no direct contact between IIP. Herewith, there appears a problem of a reliable remote identification, which is especially important in the ODR process.

In this section an attempt to work out requirements for a reliable IIP identification is given. In the ODR process participants can be: plaintiffs, defendants, neutral parties, ODS platforms operators, ODS services providers. The identification requirements are to be unified for all of them and clearly determined.

In order to work out the requirements for a reliable identification on a system basis it is necessary to state system's primary elements ensuring IIP identification when performing transactions. These components can be as follows:

- A set of identification characteristics, by which an IIP can be described in a formalized way, for purposes of a remote identification – *an identifier*;
- *An identification mean*;

¹⁹ An asymmetric encryption in the pure state is applied for a session keys encryption only due to its labour intensity, a combined encryption is the most common. An asymmetric encryption is used for session keys and a symmetric one – to encrypt a document itself.

²⁰ We mean such materials as general information about an RS operator (organization name, requisites, contacts), as well as some reference materials connected with RS functioning.

²¹ It means that register system records are readable on the service.

²² It means that register system records are readable on the service.

- *An access service operator*²³.

For ODR identification systems we can point out *a model process of access to information resources*, consisting of the following stages:

1. An assigning of an adequate identifier to an IIP prior to some information transaction.
2. A registration of an IIP identifier in an RS and/or in an access service operator's information system.
3. An RS grants an IIP an access to performance of information transactions through correlation of an identifier presented by an IIP with the one registered in respect of this IIP. This stage includes:
 - **Identification** – a participant presents an identifier in a system;
 - **Authentication** - verification that an identifier belongs to the participant presenting it;
 - **Authorization** – a granting of certain access rights to a participant.
4. A regulated fixation of access procedure results in an RS and provision of information about access events.

²³ As applied to the ODR processes, access service operator's functions can be performed by ODR platform operators on the decentralized basis. At the same time forming of a centralized access service operator to ensure a number of ODR platforms seems to be reasonable on the ground of convenience for users, who can be located in different jurisdictions, and unification of identification procedures regulations

5.10.1 Identifiers

ODR identifiers can be divided into two categories:

- **A property** an IIP has (appearance, a fingerprint, a voice, DNA etc);
- **An information** an IIP knows (full name, a password, an alias etc)

On the ground of purpose identifiers can be divided into:

- Identifiers for IIP's **self-identification**;
- Identifiers for an IIP's **external** identification.

In case of an external identification of a subject identifiers can be distributed (assigned) to an IIP and confirmed by an authorized²⁴ or an unauthorized operator.

Table 5 contains cumulative information about the most common identifiers.

It is evident that application of different types of identifiers and variants of access service operators' organization requires different financial costs. Therefore, for each application area it is necessary to work out such sets of identification characteristics, which on the one hand can ensure a reliable control of IIP access to performance of information transactions and on the other hand provide access services' low costs, which is to be significantly lower for IIP than transaction costs. The necessary level of access control can be determined basing on analysis of a model of threats and vulnerabilities for RS of different areas.

For instance, for ODR procedures:

- 1) An IIP self-identification only, for instance based on a nickname (alias), appears to be insufficient. It is necessary to register an IIP according to an order regulated at an authorized operator, whose varieties are as follows: an ODR platform operator – on a decentralized basis or an access service operator – on a centralized basis, created in the interests of a number of ODR platforms;
- 2) It is reasonable to subject access service operators and ODR platforms operators in part of their access procedures performance to a regulated audit by independent international auditors.

²⁴ An authorized operator means an operator whose activity is regulated by authorized bodies and is subject to an audit.

Table 5

Examples of identifiers

Identifier category	Identifier purpose		
	Self-identification	External identification	
		Unauthorized operator	Authorized operator
Information	Nick-name (alias)		
		Login + password	
		Full name	Full name + registration address
		Password phrase	
			Signature (analog)
	Internal IP-address	External IP-address	
	MAC-address		
		Domain name	
	Personal E-mail	Presented E-mail	
		One-time password	
			Phone number
		ES private key (an unqualified ES)	ES private key (a qualified ES)
		Radiofrequency characteristic of an RFID tag	
Property			Fingerprint
		Photo (appearance)	
			Retina
		Voice	
			DNA

5.10.2 Means of access

A mean of access is:

- For identifiers of *information* category - an aggregating agent (a physical carrier) of various IIP identifiers. For instance: a SIM card for a mobile phone, a protected key carrier for an ES private key, a one-time password generator etc.
- For identifiers of *properties* category – an input device or an identification information reader. For instance, a keyboard for a password input retina scanner or fingerprints scanner etc.

It is evident that the means of access, selected for use in some area, are to be harmonized with the system elements above by the following documents:

- Regulations of access service operators' activity;
- Unified requirements for IIP access to performance of information transactions in an RS;
- Rules of IIP access to performance of information transactions in an RS.

Thus, it can ensure:

- An interoperability of different RS in part of access ensuring;
- An audit in part of personal data protection requirements meeting;
- A convenience for users in different states subject to an adequate protection of their rights.

5.10.3 Attributes for division of an access to records

A division of IIP access privileges to RS records can be performed on the basis of two mechanisms:

- a **discretionary** (role) access control, based on a access control list or an access matrix;
- a **mandatory** access control, based on a security labels assignment from an ordered set of their values for each record and each IIP.

Both mechanisms add record's *extra service attributes* to an RS.

In case of a discretionary control *access matrix lines*, containing a final number of IIP identifiers and rights corresponding to each IIP (read/write/edit), are such service attributes. It is evident that only an RS operator itself can manage promptly an access matrix, and consequently, records' service attributes.

In case of a mandatory control a security label, identifying a record content's confidentiality level, is such a service attribute of a record. An access to a record is carried out on the ground of comparison of record's security label and IIP security label according to security rules. Security rules have to stipulate for absence of channels of information distribution from a higher confidentiality level to a lower one. Security labels are assigned to records by an RS security administrator. IIP security labels are assigned in a centralized way by an access service operator.

The access control and identifier application method peculiarities stated are suggested to be regarded as criteria when describing access service's performances available.

Table 6

Access service's performance

Identifier purpose	Type of access control	
	Discretionary	Mandatory
Self-identification	Light-performance	-
External identification (unauthorized operator)	Medium-1-performance	-
External identification (authorized operator)	Medium-2-performance	Heavy-performance

5.10.4 Access events logging

Access events logging can also have different performances: from log-files and to making regulated records in specialized service register systems. The approach is similar to the approaches to all the elements above and is based on the principle of technical neutrality that implies indicating in normative documents a necessity of a regulated access events logging.

5.10.5 Key tasks

The above description of IIP identification system's basic elements when performing information transactions in an RS enables to pass to a defining of primary tasks (requirements), first of all in a legal field, not in technological one:

I. It is required to ensure IIP characteristics authenticity and IIP personal data protection. Regulation of activity of operators working with such personal data and an independent international audit of access service operators are to be the mechanism of this requirement's implementation.

II. It is necessary to indicate capability to provide an access service in both centralized performance (based on specialized operators) and decentralized performance (based on a combination of access procedures with RS primary tasks).

III. In case of access service's centralized performance in order to ensure interoperability it is necessary to:

- 1) Work out unified requirements for IIP access to performance of information transactions in an RS;
- 2) Work out rules of IIP access to performance of information transactions in an RS.

6 Examples of the common infrastructure services implementation in different subject areas

An information process in an RS of each subject area has its peculiarities. In each subject area there exist peculiar requirements for information security (confidentiality, integrity, accessibility) provision. This Methodology is not intended to elucidate all existing nuances. The drafters just intended to suggest an approach (an algorithm), by which guiding certain subject areas specialists could select such *a set of common infrastructure service' performances* that would be sufficient to provide information processes and which would be cost-effective, when applied.

As examples of different subject areas RS the authors propose to consider:

- Supervisory bodies register systems;
- Medical RS;
- Educational RS;
- Legal regulation RS;
- Business RS.

6.1 Supervisory bodies register systems

Supervisory bodies' RS on checkpoints²⁵ is a typical practical example of **on-line** RS. Procedures' content in such check RS is approximately as follows.

1. A subject's (natural person's or legal entity's) right, for instance, some goods transport quota, is registered in an authorized body in a respective valid way. An organized aggregate of such rights is placed as records in data bases at a certain public network resource. A separate access to this data is organized for persons being supervisory bodies' representatives on checkpoints.
2. At a checkpoint a carrier presents permits, in paper form, as a rule. In compliance with regulations a supervisory body's representative is to make sure of their authenticity, for which purpose it gains access to a respective resource and gets confirmation (or records quota exceeding, for example)
3. Verification results lead to legally significant action's performance – to let the transport pass or to refuse it to pass. The action performed is recorded in the information system.

Passport control at the frontier or transport vehicles and drivers check on the road by policemen is organized on the basis of nearly the same logic. Even wider – it concerns different certificates, licenses, accreditations and other types of permits

²⁵ Customs, frontier, sanitary, veterinary, migration, transport and other control types.

that, collectively, are subjects of national electronic government construction and international information systems of a supervisory type.

A supervisory body RS essence is that a **right is reflected in a centralized core – a data base**, and an applicant physically receives a document to be presented to a supervisory body representative, who in his turn is to have an opportunity to verify presented document's authenticity on-line. For a supervisory body representative (a customs officer, a border guard) such activity has regular character, which is a differential characteristic of an **on-line** class RS.

Let's consider a process of supervisory body preliminary informing by a consignor and a sequential control at a checkpoint as an example (see Table 7).

Table 7

An example of a common infrastructure services set for ensuring of information processes of preliminary informing and sequential control at the checkpoints

	Common infrastructure services	Service performance selection
Documentation services	Signature service	In this information process ES verification is carried out at a minimum at two stages: 1. At the preliminary informing stage an RS user's (a consignor's) ES is verified. 2. At the checkpoint control stage an RS officer's (an authorized person who filled the quota) ES is verified. Since there is an intensive on-line interaction of checkpoints and CA, it is reasonable to use the Medium-1 service's performance or higher, for it implies the burden allocation and higher service reliability in whole.
	Time service	The preliminary informing time and the checkpoint control passing moment are to be certified for legal action purposes ²⁶ . Consequently, the service's Heavy-performance is required.
	Notary service	Necessity for the service's application is not evident.
	Apostil service	Necessity for an apostil service application arises in case the signature service's Heavy-2-performance is used and in case an LSMS Heavy-2-performance is used. Herewith, it is reasonable to select the apostil service's Heavy-performance for it is capable to ensure a high intensive on-line interaction.
	Location service	Forming of an attribute containing a record's performance place is acceptable using the service's Light-performance . An applicant is supposed to apply to a control RS of his jurisdiction. And, consequently, the RS itself will be a record's performance place indicator.

²⁶ For instance, Article 191 of the Commercial Code of the Customs Union states that a person submitted a customs cargo declaration may alter/amend it before the customs inspection time is appointed.

	Common infrastructure services	Service performance selection
	Legal status monitoring service	A forming of an attribute containing an applicant's legal status requires using of the service's Heavy-1-performance or higher. Such a necessity arises because of fraud commitment possibility (for instance, in case after an employee is fired). Besides, if a customs broker participates in an information interaction, he can fill in documents on behalf of different applicants, herewith, having different powers. This performance will enable to carry out an operative management of such powers.
Additional services	Payments security service	Since the number of CA and services a user interacts with is not great, the service's Light-performance is acceptable.
	Trusted data storage service	Among supervisory systems there are systems processing personal data (for instance, passport data), that results in necessity to ensure higher requirements to data safety, which the service's Heavy-performance can meet.
	Information service	Register system's records are not to be published. For reference and informational materials placing the Light-performance is sufficient.
	Access service	Taking into consideration supervisory system's importance and a high probability that defective files appear, the access service's Medium-performance or higher level should be used.

6.2 Medical register systems

Medical register systems based on citizens' medical history sheets are a typical practical example of **off-line** RS. The essence of these RS is approximately as follows

1. Some data base, associated with a subject of law (a patient), is periodically appended with records²⁷ signed by an RS officer (an attending doctor).

²⁷ The records can be as follows: complaints, analysis results, diagnosis, treatment process, treatment results etc.

2. Such subject data bases are stored in a regulated form in a medical establishment, which is responsible for its safety.
3. These data bases are periodically applied to by these information systems' staff members – doctors in a course of observing the patients. These records acquire special validity rarely, in case of a conflict only, for instance, in case of a claim by a patient or his/her relatives. Treatment correctness is verified by a respective expert medical committee. A verdict is passed on the ground of a patient history.

Medical history sheets are not published; there is no need to monitor the records regularly. Therefore, such an RS consists of a core generally; only certain extracts can be physically given to a person in question – unlike, the control systems where a record's performance is duplicated by documents, with certificates physically given to a person in question.

Let's consider a process of patient history appending and extracts from this history received as an example (see Table 8).

Table 8

An example of a common infrastructure services' performances set for providing information processes at patient history appending and extracts receiving

	Common infrastructure services	Service performance selection
Documentation services	Signature service	Making of a new record into a patient history in most cases is based on a patient's checkup by a doctor (using video communication in case of urgency). Thus, use of ES certificates issued by a CA is unnecessary. Higher requirements for an ES security are advanced only to the attending doctor's ES, by which he validates a record made. Since such machinations as "disability selling" take place, when a patient's medical report is appended with another person's checkup data, requirements for the service are to be higher; consequently the Heavy-1-performance or higher is required.
	Time service	The record making time is evidence in legal action – therefore, the service's Heavy-performance is required.
	Notary service	Necessity to use the service is not evident.
	Apostil service	The service can be used when a patient applies to a medical establishment of another jurisdiction (for example, when a person is on vacation abroad and applies to a doctor). In this case the doctor can have an opportunity to make a record to the patient history, but his ES is to be validated by an apostil service operator's ES. Such a situation does not arise often; therefore the service's Medium-1-performance is sufficient.
	Location service	A forming of an attribute containing record's performance place is acceptable with application of the service's Light-performance . A patient is supposed to apply to a medical RS of his/her jurisdiction mainly. If he/she applies to foreign doctor, then the doctor's ES attributes will be a record's performance place indicator.
	Legal status monitoring service	Since in the case under consideration records can be made into a patient history by doctors – by subjects of different jurisdictions, then there is to be an operator liable for their powers (confirming their qualification)

	Common infrastructure services	Service performance selection
		Consequently, a necessity to use the service's Medium-performance or higher arises.
Additional services	Payment security service	Since medical services payment is germane to an interaction with insurance companies, social insurance funds, with different benefits granted, the service's Heavy-performance is required.
	Trusted data storage service	Subject's health data refers to the highest category of personal data, which the higher security requirements are imposed on. The service's Medium-performance with a strict access separation mechanism can meet these requirements.
	Information service	RS records are not to be published. For reference and informational materials placing the Light-performance is sufficient.
	Access service	In this case there can be accumulation of a large volume of data critical in respect of security, which this register system's user (a doctor, a hospital administrator etc) can gain access to. Therefore, the service's Medium-1-performance or higher is required.

6.3 Educational register systems

Generally, educational information systems refer to **off-line** register systems. The following characteristic features can be singled out:

1. Accumulation of data in proportion to an education process.
2. Information systems' operators and operators' counterparties (students) periodically apply to these records.
3. Records access in case of a conflict situation (takes place extremely rarely in relation to the whole volume of documents).

Let's consider a process of a student's distance education in a university as an example. In this context, the student and the university may belong to different jurisdictions. In the process of education a grade report sheet is kept and at the end of education course a diploma of higher education is issued on the ground of this sheet (sees Table 9).

Table 9

An example of a common infrastructure services set for a provision of information processes for grade report sheet forming and diploma issuance

	Common infrastructure services	Service performance selection
Documentation services	Signature service	A distant education implies users' (students') intensive on-line interaction with RS. In this case, the user's identity is to be authenticated, which leads to necessity to apply users' ES certificates. Consequently, a necessity to use the service's Medium-2-performance or higher, arises.
	Time service	There is no need to certify the time when a record is made into a grade report sheet, therefore, the service's Light-performance is acceptable
	Notary service	A necessity to use the service is not evident.
	Apostil service	A necessity in an apostil service arises in case the signature service's Heavy-2-performance is used. At that, it is reasonable to select the apostil service's Heavy-performance , for it is capable to enable a high intensive on-line interaction.
	Location service	Forming of an attribute containing a record's performance place is acceptable using the service's Light-performance . Geographical location of a student interacting with an educational institution is not of fundamental importance.
	Legal status monitoring service	Records to a grade report sheet can be made only by personnel of an educational institution, which administers their powers independently. Therefore, the service's Light-performance is acceptable.

	Common infrastructure services	Service performance selection
Additional services	Payment security service	A student pays for his education on his own. In this framework, mutual settlements are performed with an educational institution directly. Therefore, the service's Light-performance is acceptable.
	Trusted data storage service	Every educational institution keeps a grade report list for each student and there is no necessity to organize a centralized depository. Therefore, the service's Light-performance appears to be acceptable.
	Information service	RS records are not to be published. For reference and informational materials placing the service's Light-performance is sufficient.
	Access service	A peculiarity is that while passing exams a student may be interested that another person (a better prepared student) would pass the exams instead of himself/herself. In other words, there is a rare case when a subject is interested in transferring his identifier to another subject. The subject's properties used as identifiers (see Item 5.10) can help to avoid such a situation. Therefore, it is reasonable to use the service's Medium-2-performance or higher level.

6.4 Legal regulation register systems

A system registering international, national, regional and municipal legal acts, that became effective, were amended and became ineffective (Official publication system), has both **on-line** (control, subjective-objective) system's features and **off-line** (functional) system's features. Herewith, records of such Official publication system can be accumulated while acts are passed, that is characteristic for a functional type system, and can be modified (issued, altered, terminated), that is characteristic for control systems.

An access to Official publication systems (standard ones) is to be organized **on-line**, at the same time such standard (valid) systems are inconvenient for users in practice. Therefore, private legal informational systems, having no valid information system status but herewith enabling convenient services and search interfaces for users, are formed empirically. In other words, in respect of validity

they provide an **off-line** service, which can always be re-checked in a standard data base if necessary.

Table 10

An example of a common infrastructure services set for a provision of information processes of the normative document forming and its sequential publication

	Common infrastructure services	Service's performance selection
Documentation services	Signature service	A register system operates with ES of many authorized persons who are subjects of one jurisdiction. Users (citizens) are not authorized to alter the register system's records. Authorized persons' ES certificates are to be issued by a certification authority of the same jurisdiction they belong to – therefore the service's performance is to be Heavy-1 or higher level.
	Time service	There is no need to certify the time when a normative document is formed, therefore the service's Light-performance is acceptable.
	Notary service	Necessity to use the service is not evident.
	Apostil service	Necessity to use the service is not evident.
	Location service	The document's issue place is defined by an RS jurisdiction itself. Since a certification is unnecessary, the service's Light-performance is acceptable.
	Legal status monitoring service	A document negotiation and signing process implies an ample quantity of differently empowered authorized persons' signatures to be processed. The powers can be altered quite often and are to be timely monitored. In such circumstances it is reasonable to use the service's Heavy-1-performance or higher level.
Additional services	Payment security service	Necessity to use the service is not evident.
	Trusted data storage service	A great number of users are to have access to normative documents, which means higher requirements for performance and reliability. A specialized approach, namely the service's Heavy-performance , is reasonable to be applied for storage and access granting.
	Information service	An information service is to enable search in a normative documents data base. Reference intensity can be high.

	Common infrastructure services	Service's performance selection
		Consequently, the service's Heavy-performance is required. It is evident, that the service is to function together with the trusted data storage service.
	Access service	The system can operate with documents of a special importance on both state level and international level. Therefore, the service's Medium-2-performance or higher appears to be necessary.

6.5 Business register systems

Generally, business information systems refer to **off-line** register systems. The following characteristic features can be singled out:

1. Accumulation of records in course of business operations.
2. Information systems' operators and operators' counterparties (legal entities) periodically apply to these records.
3. Records access in case of a conflict situation (takes place extremely rarely in relation to a volume of documents)
- 4.

To illustrate the common infrastructure services' application in the business sphere we propose to consider a complicated and yet unsolved question concerning release, use and transfer of *electronic transferable records* (hereinafter referred to as the "ETR")²⁸. For the purpose of the Methodology the term "electronic transferable records" means an electronic equivalent of a transferable (negotiable or non-negotiable) document or a document of title²⁹. A paper transferable document's peculiarity is that it is recognized as a unique embodiment of the rights it vests. *A physical transfer* of a paper document to an endorsee is a mechanism used to transfer rights stated in paper transferable documents. In other words, as a result of a transferable document original copy transfer to an endorsee, the latter gains a valid title to this document and the rights vested in it.

When organizing work with the ETR the main two problems to be solved are:

1. A problem to ensure a document's *uniqueness*. Its difficulty consists in the fact that an electronic record can be copied in such a way that a

²⁸ A detailed reasoning concerning the essence of the terms "an electronic transferable record" and "negotiability" are given in Supplement 2.

²⁹ The UNCITRAL document A/CN.9/WG.IV/WP.115 "Legal issues relating to the use of electronic transferable records"

duplicate record, identical to the original copy and undistinguishable from it, is created.

2. A problem to define a functional equivalent of a mechanism to meet requirements in respect of ETR *possession*, that is, a mechanism identifying a person as a holder (an endorser) in any particular time.

A solution to the problems set is proposed to be carried out using a public key infrastructure technology, herewith, an endorsement is an attributive certificate. The approach's essence is stated in the Supplement 2.

An attribute certificates' life cycle management is carried out by an LSMS in the **Heavy-performance**, with its work algorithm being analogous to a work algorithm of a certification authority, managing ES certificates' life cycle.

A proposed common infrastructure services set necessary to work with the ETR is presented in Table 11.

Table 11

An example of a common infrastructure services set for a provision of information processes when working with electronic transferable records.

	Common infrastructure services	Service's performance selection
Documentation services	Signature service	An endorser and an endorsee can be subjects of different jurisdictions; an information interaction is more intensive due to a large quantity of endorsements. Thus, it is reasonable to use the service's Heavy-1-performance or higher .
	Time service	The endorsement precise time recording has a key importance. It appears reasonable to use the Heavy-performance , whereby an operation's execution time is assured with a time service operator's ES.
	Notary service	Notary functions in the business sphere are mostly demanded. The service's Heavy-performance use is evident
	Apostil service	A necessity in an apostil service arises in case the signature service's Heavy-2-performance is used and in case the LSMS Heavy-2-performance is used. In this framework it is reasonable to select the apostil service's Heavy-performance , for it is capable of providing high intensive on-line interaction.
	Location service	Since an endorsement deed does not imply a necessity to certify an operation's performance place, the service's Light-performance is acceptable.
	Legal status monitoring service	As it is described above, an endorsement is based on the LSMS decentralized architecture utilization, which implies the service's Heavy-1-performance or higher level.
Additional services	Payment security service	Since an interaction with an LSMS is based on ES certificates utilization, it appears sound to include the LSMS services cost into the ES certificate issue cost. Consequently, it is reasonable to use the service's Heavy-performance .

	Common infrastructure services	Service's performance selection
	Trusted data storage service	Since the order above does not imply the ETR storage with a centralized operator, and attributive certificates storage and management is carried out by the LSMS, the trusted data storage service's Light-performance is acceptable.
	Information service	An information service is to enable a search by an attributive certificates data base. An intensity of references to a server can be high. Consequently, the service's Heavy-performance is required. It is evident, that the service is to function together with an LSMS.
	Access service	In the process of business electronic interaction there appears a risk of financial losses because of an unauthorized access to documents. Therefore, it is reasonable to use the service's Medium-2-performance or higher.

In conclusion we present a summary Table (see Table 12), stating the common trust infrastructure services' performances to assure the information processes in different subject areas considered above.

Table 10

A summary Table of the common trust infrastructure services' performances to assure the information processes in different subject areas

Register systems	Documentation services						Additional services			Access service
	Signature service	Time service	Notary service	Apostil service	Location service	Legal status monitoring service	Payment security service	Trusted data storage service	Information service	
Supervisory bodies RS	>M2	H	-	H*	L	>H1	L	H	L	>M1
Medical RS	>H1	H	-	M1	L	>M	H	M	L	>M1
Educational RS	>M2	L	-	H*	L	L	L	L	L	>M2
Legal regulation RS	H1	L	-	-	L	>H1	-	H	H	>M2
Business RS	>H1	H	H	H*	L	>H1	H	L	H	>M2

L – Light-performance of a service

M – Middle-performance of a service

M1 – Middle-1-performance of a service

M2 – Middle-2-performance of a service

H – Heavy-performance of a service

H1 – Heavy-1-performance of a service

H* – Heavy-performance of an apostil service in case of the signature service's Heavy-2-performance, as well as in case of the LSMS Heavy-2-performance.

As we can see from Table 12 information processes in register systems can be provided by different performances' combination. Prior to the final selection, a feasibility study of every service's performance is to be carried out. The final justification of a certain performance for a certain information process can be carried out on the ground of such analysis results and taking into account an acceptable level of trust between register systems and the common infrastructure services operators.

Conclusion

A conversion to a practical constructing of an electronic interaction in the framework of the TTS requires the system's implementation certain options to be defined.

A model register-information process characteristic for any RS and any type of information interaction is described. Herewith, this process's performance in a specific subject area was demonstrated to point out certain peculiarities.

Resulting from the analysis of a document's conversion from a paper form to an electronic one, the documentation services were singled out; their list arises from an aggregate of attributes necessary for an electronic record and an electronic document to ensure validity. Functions of separate access assurance are performed through an access service. Besides the documentation services, the access service, performing the function of a separate access to a record, exists.

In respect of the TTS it means that in every state the common trust infrastructure services' relevant operators are of function alongside with RS operators. Meanwhile, the former are to provide transboundary information interaction participants with instruments enabling to assign validity to information resources generated. Security of the resources contained in these register systems is to be assured by these systems operators.

One of the problems arisen in the process of this Methodology drafting was that each service has a number of optional performances: technological, organizational and legal. It didn't seem possible to describe the whole range of these options; therefore we decided to present the following approach to the expert consideration. We singled out two extreme cases, conventionally called Light and Heavy, and an intermediate case, that can be called Medium. The basic division criterion is a level of trust between information interaction participants.

The Light-version, characteristic for a high level of trust between information interaction participants, represents the services already existing in some cases. Systems like EDMS and IDFS can be examples of the systems fully based on the Light-requirements.

The Medium- or Heavy-requirements imply the common trust infrastructure services performance on a centralized or a decentralized principle respectively. This is the ways of new services and new information systems' components forming, implying requirements to be imposed on national RS, including already existing ones.

At centralization (the Medium-requirements) the less critical services can be assigned to a single operator that will make it possible to reduce costs for their implementation. But in this case standardization at technological, organizational

and legal levels is required. An adaptation to new technological standards by their appearance is to be consistently carried out by all the TTS participants.

The Heavy-version can comprise the services, with all performances having some decentralized execution. Such a totally decentralized performance will not only cause higher expenses but could be impossible for practical execution in the system as well.

But there is another extremity which is the overall trust, also unacceptable in the modern world, which is evident without any extra comments. The search for a “golden mean”, an optimal combination of the centralization/decentralization principles in providing trust services is the subject matter of further consideration. The present Methodology is supposed to provide necessary information for thought and the working out of decisions, without which further TTS system design can become ineffective.

In this connection the drafters prepared a respective Table (Supplement 1) to interview potential TTS participants, which is proposed to be filled in the foreseeable term. Thereafter, the results will be summarized and considered at regular meetings of the CIS RCC member-states’ Regional commonwealth in communication.

Supplement 1. A form for common trust infrastructure services performances selection

Table 11

	Common infrastructure services			Performance selection
	Service name	Performance	Brief characteristics	
Documentation services	Signature service	Light	A corporative ES	
		Medium-1	A single international CA	
		Medium-2	A national CA network; trust relations are constructed on the principle of a hierarchy with an international CA as a root CA	
		Heavy-1	A national CA network; trust relations are constructed on the principle of a cross-certification	
		Heavy-2	A national CA network; trust relations are assured by an apostil service	
		Other	Another option	
	Time service	Light	A clock is synchronized with public network time servers' clocks	
		Medium	A clock is synchronized with a common infrastructure time service's clock	
		Heavy	The time is assured with a time service operator's ES	
		Other	Another option	
	Notary service	Heavy	A decentralized service architecture	
		Other	Another option	
	Apostil service	Medium-1	An apostil service single international operator	
		Medium-2	An apostil service single international operator interacts with apostil service's national operators	
		Heavy	Apostil service's national operators interact directly	
		Other	Another option	
	Location service	Light	Attribute's value is set by a register system itself	
		Medium	Operation performance location is assured by a notary's ES	
		Heavy	Operation performance location coordinates are assured by a service	

Common infrastructure services			Performance selection		
Service name	Performance	Brief characteristics			
		operator's ES			
		Other	Another option		
	Legal status monitoring service	Light	A legal status is managed by a register system operator itself		
		Medium	A subject's legal status is stated in his ES certificate		
		Heavy-1	A subject's legal status is stated in an attributive certificate; trust relations between service operators are constructed on the principle of cross-certification or hierarchy		
		Heavy-2	A subject's legal status is stated in an attributive certificate; trust relations are assured by an apostil service		
		Other	Another option		
	Additional services	Payment security service	Light	Mutual settlements between a subject and a register system's operator are direct	
			Heavy	Services cost of service utilization are included into a cost of a subject's ES certificate	
			Other	Another option	
Trusted data storage service		Light	Data is stored locally in each register system		
		Medium	Data is stored locally in each register system. Data access is performed with application of a legal status monitoring service		
		Heavy	Data is stored in a trusted storage service. Data access is performed with application of a legal status monitoring service		
		Other	Another option		
Information service		Light	Static materials are published by a register system's operator itself		
		Medium	Dynamically altering materials are published by a register system's operator itself		

	Common infrastructure services			Performance selection
	Service name	Performance	Brief characteristics	
		Heavy	Dynamically altering materials are published by an information service's operator. Higher access requirements are assured	
		Other	Another option	
Access service		Light	Self-identification. Discretionary access control	
		Medium-1	External identification (unauthorized operator). Discretionary access control	
		Medium-2	External identification (authorized operator). Discretionary access control	
		Heavy	External identification (authorized operator). Mandatory access control	
		Other	Another option	

Contacts:

- **Alexander Sazonov**, tel.: +7 (495) 690-92-22 (add 402),
e-mail: sazonov@nucrf.ru;
- **Georgiy Vuss**, tel.: +7 (499) 235-62-65,
g.vuss@mail.ru
- **Vladimir Kustov**, tel.: +7 (812) 520-30-50 (add 1703),
Kustov-V@gaz-is.ru

Supplement 2. Application of common trust infrastructure services for endorsement assurance

This supplement justifies the term “an electronic transferable record”, demonstrates its correlation with a concept of a document’s negotiability and illustrates a principle capability to assign rights stated in a bill of lading via the common trust infrastructure.

The primary task of a document is to assure a legal function. Let’s consider documents conferring some rights of a particular person. Rights stated in a document can be assigned to a person *once*, as in case a citizen’s passport is issued, or transferred from one person to another *repeatedly*, as in case of a negotiable bill of lading. In both cases a document possession is a necessary condition for possession of a right it vests. Thus, uniqueness is a key property of a document alongside with its integrity and authenticity³⁰. As of today, paper document uniqueness is assured by a great number of organizational and technical measures taken in the framework of a relevant legal environment. Herewith, an understanding of a document as a copy (or, an *exemplar*) – as a self-sufficient essence is a pillar stone underlying legal, organizational and technical issues concerning a paper document’s life cycle. Naturally, any document can fulfil its legal function only in a particular legal environment. But a legal environment itself is an aggregate of such documents, but of a higher legal tier. At the same time, working with a document implies arranging of a peculiar legal succession, which includes documents from the lowest level to the highest one. In case of paper documents forming of such a succession and its verification on the ground of a final subject’s particular right requires significant labor and time costs, and real time mode verification is impossible.

A special value of modern information technologies in this aspect consists in availability to verify and manage subject’s right in a *real time mode*. Herewith, subject’s rights are reflected in *records* in data bases of register systems, while their operators are responsible for management of a particular category of rights. Thus, a *record* in a register system data base performs a task of *legal function assurance*, and rights assignment between subjects can be regarded as a *transfer* of this record. From this point of view use of the term “an electronic transferable record” seems to be appropriate. Generally, the term “a transfer” in respect of a

³⁰ A confidentiality property is important as much, but in the document type under consideration it doesn’t have a key role.

record is quite conventional, as well as concept of a record *possession*. In this context, issues of record access providing and separation come to the forefront.

A paper document's negotiability as a matter of fact is *an assignment of rights* vested in this document, through a physical transfer of this document from one subject to another. Actually a citizen's passport (or another identity document) can be regarded as a *once negotiable* document as well – citizen's rights are once transferred from an authorized body to a person.

When we speak about an electronic record, assignment of a right it vests is performed through *a transfer of a control* of it from one subject to another.

A single right assignment is the easiest to realize because when a record is processed, a register system's operator interacts with one particular subject, whereby the latter is not entitled to assign his rights to another subject (a citizen's passport transferred to another subject does not grant the latter with civil rights).

A repeated rights assignment requires a more complicated mechanism to be used, for a record access is to be granted to different subjects in different periods of time.

Let's consider how a case of a repeated rights assignment, namely a rights assignment via *a to-order bill of lading*³¹, can be performed with application of the common trust infrastructure services in the paradigm described.

An approach suggested is based on application of a *public key infrastructure* technology. The approach essence consists in the following.

An endorsement is an attributive certificate containing the following data³²:

- identification data of the attributive certificate itself³³;
- hash value (hereinafter referred to as "hash") of a bill of lading content;
- identification data of an endorser's ES certificate³⁴;
- identification data of an endorsee's ES certificate.

Hash of a bill of lading content assures its integrity while ES certificates identification data univocally identifies an endorser and an endorsee.

A rights assignment process consists in a nullification of an attributive certificate and in issue of a new attributive certificate containing ES certificate's identification data of a new rights holder.

³¹ Article 148. Commercial navigation Code of the Russian Federation dated April 30, 1999 N 81-FZ

³² The list given cannot purport to be complete (and can be added if necessary). It seems to be sufficient to assure a rights assignment process in the common trust infrastructure.

³³ Attributive certificate's identification data means data about the operator who issued it and this operator's number unique within the register system.

³⁴ ES certificate's identification data means data about the CA which issued it and an owner of the certificate.

Attributive certificates' life cycle management is performed by a centralized or a decentralized operator, whose work algorithm is analogous to a work algorithm of a certification authority, managing an ES certificates' life cycle. In case of a decentralized operator's interaction scheme, as well as in case of certification authorities, trust relations between operators can be constructed on the principle of a cross-certification, hierarchy or with application of an apostil service.

A rights assignment process consists in the following.

1. An endorser forwards an enquiry for an endorsement signed with his ES to an operator. This endorsement contains:
 - identification data of the attributive certificate corresponding to the current endorsement;
 - identification data of an endorsee's ES certificate.
2. An operator carries out the following verifications:
 - a. verifies an endorsee's ES on the enquiry for an endorsement;
 - b. on the ground of the attributive certificate's identification data stated in the enquiry for an endorsement searches for this attributive certificate in a data base.
 - c. verifies correlation of identification data of an endorser's ES certificate in the attributive certificate with the identification data of the ES certificate the enquiry for an endorsement is signed with.
 - d. verifies the attributive certificate's validity:
 - i. verification of an ES of an operator's authorized person who issued the attributive certificate;
 - ii. verification of a validity period stated in the certificate;
 - iii. verification of the attributive certificate using a list of attributive certificates nullified.
 - e. by accessing to other operators' data bases verifies absence of the attributive certificates (both valid and nullified) containing the hash of a bill of lading content identical to the hash stated in the attributive certificate.
3. In case the verification results are positive the operator nullifies the current attributive certificate (enrolls this certificate to the list of certificates nullified) and issues a new attributive certificate, containing hash of a bill of lading content and identification data of an ES certificate of the endorsee the rights are assigned to.

This process has two weak points:

1. The verification stated in the point “e”, assuring an endorsement’s uniqueness. An optimization of this verification can consist in division of operators according to bills’ of lading types (or according to types of rights they vest), for which they assure attributive certificates’ (endorsements’) life cycle.
2. A vesting of rights in a bill of lading is to be performed in compliance with strictly determined syntactic rules in such a way that it is impossible to describe the same legal relations with different syntactic constructions. This problem can be solved by use of a functional of a register system³⁵ enabling to draw up a bill of lading through filling in (selecting of values) of a certain number of interactive forms.

Advantages of the approach described are as follows:

1. A capability to identify a possessor of a bill of lading by a corresponding attributive certificate in any particular time moment.
2. An application of a wide spread mechanism of an endorser authentication, based on an application of his ES certificate.
3. An attributive certificate connects a bill of lading and an endorser. Herewith, an attributive certificate’s uniqueness and integrity can be assured by means widely used in the certification authorities’ work.

The rights assignment process description above is not comprehensive – it doesn’t include conventional transfers in case of verifications’ negative results. Besides, the process can include extra operations/verifications connected with peculiarities of a rights assignment via a bill of lading. The primary task of the description presented is to illustrate a principal possibility to assign rights stated in a bill of lading via the common trust infrastructure services in general and attributive certificates technology in a particular.

³⁵ A bill of lading drawing up functional and attributive certificates’ (endorsements’) life cycle management functional can be combined in a single register system or divided to different register systems.

Supplement 3. Comparative analysis of the UNCITRAL document A/CN.9/WG.IV/WP.115 and the TTS Model

The Model of the CIS member-states transboundary common trust space's forming and functioning in the Internet network (the TTS Model), which the present Methodology is based on, has intersections of a number of issues concerned in the UNCITRAL document A/CN.9/WG.IV/WP.115 "Legal issues relating to the use of electronic transferable records".

This document considers problems arising in the process of electronic transferable records utilization. Regardless that the document is drafted in frames of a specific subject area (foreign trade), it has general points partially presenting in the TTS Model.

For more obvious demonstration it is reasonable to draw up a Table of correlation of the TTS Model's wordings with the ones used in the UNCITRAL document (Table 12).

Table 12

Comparative Table of the wordings used in the UNCITRAL documents and in the TTS Model

	Wordings used in the UNCITRAL document A/CN.9/WG.IV/WP.115	Wordings used in the TTS Model
Electronic transferable records	<p>The term electronic transferable record is used in this note as a general term to refer to the electronic equivalent of a transferable instrument (negotiable or non-negotiable) or a document of title... (art. 3)³⁶</p> <p>To distinguish an electronic transferable record from its paper equivalent, the term "transferable paper" is used in this note as a general term to refer to transferable instruments and documents of title in traditional paper form (art. 5)</p>	Electronic Transferable Records – a type of electronic documents recorded in register systems, based on the common infrastructure of information documentation in electronic form

³⁶

A reference to an article in the document A/CN.9/WG.IV/WP.115.

	Wordings used in the UNCITRAL document A/CN.9/WG.IV/WP.115	Wordings used in the TTS Model
Definition of an authoritative copy	An alternative approach allows the specific copy that constitutes the authoritative copy, and the computer system on which it is stored, to change over time. This is often done through the use of a registry that tracks the location where the authoritative copy is stored, and/or that maintains a digital fingerprint (e.g., the hash value or digital signature) of the authoritative copy so that it can be readily determined whether the integrity of the copy maintained by or for the holder is intact and matches the original. Sometimes referred to as a registry model, this approach allows for the creation, issuance, storage and transfer of the electronic transferable record on a variety of distributed information systems, with certain information transmitted to and recorded in a central registry. The designated authoritative copy of the electronic transferable record is not necessarily stored in the registry, but any copy can be verified as accurate by reference to the registry (art. 40 b)	A permanent separate access to electronic transferable records is to be provided (an on-line mode). Extracts in a form of electronic documents, which can be valid off-line, can be issued on the ground of electronic transferable records. Herewith, after some period of time regulated they can be confirmed either through accessing to current register systems or by receiving of current extracts from these register systems
Registry model	A registry model allows for the creation, issuance and transfer of electronic transferable records based on information transmitted to and recorded in a central registry. Access to the registry might be controlled and might be subject to acceptance of contractual provisions (art. 52)	Electronic transferable records' forming, storage and termination of validity is to correspond to rules and requirements for electronic information documentation, whereby register systems as well as the common infrastructure or its individual components (services) are to be managed by authorized or trusted operators, whose activity is subject to an audit.

	Wordings used in the UNCITRAL document A/CN.9/WG.IV/WP.115	Wordings used in the TTS Model
Further work directions	... it might be useful to develop a clear set of high-level principles to be incorporated in any international system for electronic transferable records. Such principles will need to address issues relating to transboundary use of electronic transferable records, too (art. 65)	A detailed description of all the TTS components, units, services and modules and description of information interaction participants' rights and obligations as well as other legal issues of a transboundary information interaction can be performed in the framework of the second and third stage of the TTS system forming with provisions of the Model approved to be taken into account.

After analyzing the Table the following conclusions can be drawn:

1. Both documents consider issues of application of electronic transferable records as a type of electronic documents. But in the TTS Model the concept of an electronic transferable record has a wider meaning, comprising the UNCITRAL experts' understanding of this term as well (see Supplement 2).
2. In the TTS Model an issue of electronic transferable record copy's authentication definition is suggested to be solved through granting of an access to relevant register systems. In the A/CN.9/WG.IV/WP.115 such approach is called "alternative" and implies using of a certain register, which, being applied to, enables to verify an exactness of any electronic transferable record's copy.
3. The UNCITRAL document describes a necessity of a system of registers, where electronic transferable records can be released and transferred. Analogously, the TTS Model provides for register systems based on the common documentation infrastructure and performing similar functions. Herewith, in both cases a regulation of such systems operations is provided.
4. Further TTS Model's performance stages are directly connected with work guidelines of the Working group IV in regard of electronic transferable records utilization principles.

Thus, we can say that the ideas used in the TTS Model and their performance methods, suggested in the present Methodology, correlate with the current issues considered by international organizations, the UNCITRAL Working group IV, in particular.