

Recommendation for ensuring legally significant trusted transboundary electronic interaction

CONFERENCE CALL
September 4, 2015

Attendance

Present:

Aleksandr Sazonov (RU)
Anna Nordén (SE)
Dmitry Iakymenkov (UA)
Igor Furgel (DE)
Ramachandran P. (IN)

Absent:

Alexey Domrachev (RU)
Anders Tornqvist
Andrea Caccia
Angelo Tosetti (IT)
Anne Sandretto (FR)
Antonio Petrella
Bassil Eid (FIATA)
Bill Luddy (US)
Bud P. Bruegger (DE)
Carlo Salomone (IT)
Eric E. Cohen (US)
Jari Salo (FI)
Jean-Michel Kaliszewski (IATA)
João Rodrigues Frade (European Commission)
Lauri Railas (FI)
Lance Thompson (US)
Maria Ceccarelli
Margo Tank (US)
Moudrick M. Dadashov (SE)
Prianceu Pandey (IN)
Richard L. Field (US)
Susanne Wigard (DE)
Tom Smedinghoff (US)
Viky Manaila
Yuriy Kharakhordin (EAC)

General summary – overview

- **Members welcome.**
- **Term “transboundary trusted added.**
- **Mandatory and optional attributes of an electronic document.**
 - It was preliminary agreed to make mandatory the following attributes: 1) content; 2) signatory status; 3) signature; 4) time.
 - It was suggested to consult with absent experts.
- **Trust service providing identification of legal and natural persons**
- **Long-time archival and verification service**
 - It was agreed this service’s function is to verify validity of a document at a moment in the past.
 - It was agreed to state this service as “long-time archival and related verification service”.
- **Communication with UNCITRAL on legal regulation**
- **Summary**
 - It was agreed to work out Foreword and the section dedicated to communication with organizations on standardization on a technical aspect.
 - It was planned to prepare a final draft for a public review at the forum.

Detailed summary of each agenda item

Topic	Comments
<p>Foreword</p>	<p><u>Alexander Sazonov</u>: What information should the Foreword part contain?</p> <p><u>Igor Furgel</u>: There should be just 1-2 sentences the status of this Recommendation and that it is issued by CEFACT - some formal information.</p> <p><u>Alexander Sazonov</u>: We should state there who this Recommendation is addressed to.</p> <p><u>Igor Furgel</u>: Agree. What this document is and who is the expected audience.</p> <p><u>Alexander Sazonov</u>: I will add it to the next draft revision.</p>
<p>Executive summary</p> <p>The general purpose upheld by this Recommendation is to guarantee ensuring rights and legal interests of citizens and organizations under the jurisdiction of United Nations Member States while performing legally significant information transactions in electronic form using the Internet and other open ICT systems of mass usage.</p> <p>This institutional guarantees are proposed to be ensured within business activity of specialized operators which:</p> <ul style="list-style-type: none"> - provide users with a set of trusted ICT services; - operate within established legal regimes, which include but are not limited to restrictions imposed by processing of personal data. <p>Current Recommendation covers only the provisions concerning trusted ICT services. Provisions regarding establishing appropriate legal regimes may be subject matter of a dedicated Recommendation by UNCITRAL.</p> <p>Any participants of electronic interaction deal with some kind of ICT services (email, cloud storages, web-portals etc.). If participants have a high degree of confidence in each other and in ICT services they use, then nothing is to be changed. But if participants are not sufficiently confident in each other and/or in ICT services, then there should be a third party increasing the degree of confidence in electronic interaction on the whole. The role of these third parties play trust services.</p> <p>Trust services may be of different types (provide different functions) and of different levels of qualification. High level qualification trust services operates under some international legal agreements, they meet the requirements and follow the rules laid down by some international coordinator. Basic level qualification trust services operates under some commercial agreements, they can be established within some large scale international projects and follow the recognized best practices for trust service providers. Trust services should be audited in accordance with their level of qualification.</p> <p>The aggregate of trust services with the legal, organizational and technical framework forms the Common Trust Infrastructure (hereinafter CTI). The CTI is a fundamental, easily</p>	<p><u>Alexander Sazonov</u>: During the April Forum in Geneva TTP experts advised to prepare a short high-level description of the Recommendation that would be understandable to the public. It is merely a description of what the following text deals with.</p> <p><u>Anna Nordén</u>: The introduction is quite relevant and helpful.</p> <p><u>Igor Furgel</u>: I agree, this part is useful for understanding of the text.</p>

scalable infrastructural platform providing a unified access to trust services.

2.1 Terms and Definitions

transboundary trust space (TTS)

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

Alexander Sazonov: We added a term “transboundary trusted space”, since it is used further in the text. It is a high-level description, and I think it fits the idea of the draft.
(No objections)

2.4 (attributes)

No	Attribute type	Mandatory yes/no	Description/comments
1.	Content	yes	An aggregate of at least one of the following attributes is the <i>content</i> , the informational essence of a document, which is to be irrespective to an expression form – whether paper or electronic one: 1) document type 2) document classification 3) document title 4) table of contents 5) document body (mandatory) 6) annexes Herewith, information integrity and authenticity are to be assured when processing, storing and transferring.
2.	Document issuer legal status	yes	An aggregate of the following attributes is the <i>document issuer legal status</i> : 1) logotype 2) name of a issuer 3) issuer reference data (address, contacts etc.) 4) seal impression It can be performed through constituting of an authorized body that provides electronic register assuring the attribute validity property. or For electronic seals it can be fixed with a special attribute in electronic seal certificate.
3.	Signatory status (powers) or signatory position	yes	Can be performed through forming of an electronic register of authorized persons or roles, containing a brief description of powers with their duration stated. or Can be fixed with a special attribute in electronic signature certificate.
4.	Signature	yes	An aggregate of the following attributes is the <i>signature</i> : 1) issuer’s signature 2) signature stamp of confirmation 3) signature stamp of approval 4) visa (clearance / endorsement stamp) 5) copy certification stamp 6) electronic seal of issuing organization 7) etc.

Alexander Sazonov: We added an attribute to the table of the attributes required for document’s legal significance. We discussed earlier that there should be a set of such attributes and consulted with our experts on the issue which attributes are mandatory and which are not. We suggest adding an attribute named “Place” indicating geographic location of the signatory, because in some legal regimes it is necessary. Though currently we have no special advice how it can be technically implemented, I think there are technical solutions based on global satellite services. We added this attribute just in order to show that it should be but we don’t concretize the particular technical solution, it is up to our colleagues from ISO, ETSI. All the attributes listed in the table should mandatory for worldwide document exchange.

Igor Furgel: No objections.

Anna Nordén: Generally I agree. But I wonder if it might be problematic to state that something is mandatory.

Alexander Sazonov: we should decide whether a document transferred in the cross-border

			<p>Can be performed through using of an electronic signature (for natural persons) and/or electronic seal (for legal entities).</p> <p>Note: The form of the relationship between the signatory and the document content (negotiation, approval, visa, copy legalization, etc.) can be stated in a document body, included to an electronic signature/seal or reflected in metadata to a record in an electronic data base.</p>	<p>scenario must have a minimum set of attributes and what attributes it must be. Or in some cases there will be only two attributes, for example, content and signature. What should we make mandatory and what – optional.</p> <p><u>Dmitry lakymenkov</u>: I think for now signature will be enough.</p> <p><u>Alexander Sazonov</u>: At least one more is required – the content, because you must sign something.</p> <p><u>Dmitry lakymenkov</u>: From semantic point of view you are right, but according to national law only one attribute is mandatory.</p> <p><u>Igor Furgel</u>: At least three attributes are mandatory: 1) content; 2) signatory status; 3) signature. It is important to determine the signatory status when the document was signed.</p> <p><u>Alexander Sazonov</u>: Thus, we make mandatory: 1) content; 2) signatory status; 3) signature; 4) time. I suggest the following: I will address this question to our experts that are absent today.</p>
5.	Time	yes	A statement of the time point of signing, attached on the basis of a trusted time source (the validity aspect).	
6.	Place	no	<p>A statement of the place of signing (the place where Signatory expressed his/her will to sign by triggering signing) is optional. There would be at least a theoretical opportunity for TSPs for offering – similarly to the time stamp service - a ‘place stamp service’ based on a trusted geo position source (e.g. a global navigation satellite system (GNSS)).</p> <p>If this type of service is not available the attribute <i>place</i> can be considered as one of the <i>content</i> attributes.</p>	
<p>Trust service providing identification of legal and natural persons</p> <p>a) Providing identification of natural or legal persons.</p> <p>The following attribute types (see Ошибка! Источник ссылки не найден.) presume a previously performed identification of related natural or legal persons:</p> <ul style="list-style-type: none"> - document issuer legal status; - signatory status (powers) or signatory position; - signature. <p>The trust service types a) and b) use these attribute types and, hence, also presume a previously performed identification of related natural or legal persons. The identification services are provided by operators specialized in performing identification. These services can be implemented on different qualification levels: zero, basic and high. The ICC shall decide/agree on eligible identification schemes including minimal requirements on them.</p>				<p><u>Alexander Sazonov</u>: we added to this section concerns a new service type. It is a trust service providing identification of legal and natural persons. It is necessary because other trust services deal with identity and authentication of persons. In this connection a few aspects should be considered:</p> <ul style="list-style-type: none"> - Service qualification

<p>There may be ICC own identification schemes and/or references to international standards and/or references to the notified identification schemes inside the single trust domains.</p> <p>Sets of identification attributes and identification procedures themselves can serve as the basis for the definition of the qualification levels of identification schemes. The qualification levels of identification schemes can be of essence for the regulation of interaction between different trust domains. Sets of identification attributes can be defined by the legal regimes for the business activity of operators specialized in performing identification and of functional operators. Sets of identification attributes can be maintained by the trust services (identification service). The activity of operators specialized in performing identification can be regulated by special organizational and technical requirements directed, besides others, on personal data protection.</p>	<p>(zero/basic/high);</p> <ul style="list-style-type: none"> - Sets of identification attributes. They can be regulated under national legal regimes or by an international coordination council. In any case they are to meet certain requirements depending on the service qualification. - This service should operate within a national legal regime and be a part of a national identification scheme. (No objections)
<p>Long-time archival and verification service</p>	
<p><i>Note. Long time archival and related verification service can be realized as a function of ICT service or as a function of a special trust service type.</i></p>	<p><u>Alexander Sazonov</u>: The next point concerns long-time archival and verification service. We consider that long-time archival should be a function of an ICT service used by participants. Or it may be a special trust service type if it is needed in the future. But it doesn't relate to the subject matter of this document).</p> <p><u>Igor Furgel</u>: I agree. It should be detailed in a special document.</p> <p><u>Dmitry Iakymenkov</u>: Do you mean verification service relates to this archive or any document?</p> <p><u>Igor Furgel</u>: I think it concerns the long-time archival.</p> <p><u>Alexander Sazonov</u>: Yes, it deals with verification of a document in long-time archive. Its function is to verify validity of a document at a moment in the past.</p> <p><u>Dmitry Iakymenkov</u>: In this case it should be considered together with LTA. May be better describe it more clear.</p>

	<p><u>Igor Furgel</u>: Perhaps, it should be stated as “long-time archival and related verification service”.</p> <p><u>Alexander Sazonov</u>: I agree.</p> <p><u>Dmitry Iakymenkov</u>: Agree.</p>
Communication with UNCITRAL on legal regulation	
<p>1) It is recommended to give a description of different possible legal regimes:</p> <ul style="list-style-type: none"> – based on international agreements (conventions) and/or on directly applicable international regulation; – based on commercial agreements and/or common trade practice; – without special international regulation. <p>Legal regimes can be additionally supported by traditional institutes (governmental authorities, judicial settlement, risk insurances, notary ship and others) through mutual recognition of electronic documents secured by trust services.</p> <p>Established legal regimes can also provide for imposing special requirements on the material and financial support of the business activity of specialized operators in case of damage to their users, including cases of compromising personal data.</p> <p>Issues of institutional guarantees and legal regimes for constituting and functioning regional and global TTS-domains are proposed to be considered in a separate UNCITRAL Recommendation.</p> <p>2) It is recommended to describe the mechanisms of interaction of particular states and their international unions with other international formats in the frames of constituting of a common TTS:</p> <p>2.1) By means of the complete or a partial joining a state to an existing legal regime on the basis of international treaties and/or directly applicable international regulations, in which frames a task on forming a regional TTS has already been set or solved. This existing legal regime ensures institutional guarantees to the subjects of electronic interaction.</p> <p>2.2) On the basis of interaction between different international unions:</p> <ul style="list-style-type: none"> – in the first stage, a group of states creates an regional TTS domain ensuring institutional guarantees for the subjects of electronic interaction within the legal regime specified by these states; – in the second stage, the protocols of trusted interaction with other international unions are specified as related to mutual recognition of different legal regimes. This mutual recognition shall regard to institutional guarantees and information security requirements appertaining to each of the international formats, possibly on the basis of a nIDG being operated in the frames of an international legal regime. <p>2.3) On the basis of interaction of a state with other states or international unions:</p> <ul style="list-style-type: none"> – in the first stage, a state creates its own trust domain functioning in the frames of national legal regime specified by this state; – in the second stage, the protocols of trusted interaction with other states and/or international unions are specified as related to mutual recognition of different legal regimes. This mutual recognition shall regard to institutional guarantees and information security requirements appertaining to these states and international formats, possibly on the basis of a nIDG being operated in the frames of an 	<p><u>Alexander Sazonov</u>: We added a section that concerns communication with UNCITRAL on legal regulation. There are a few levels of interoperability:</p> <ul style="list-style-type: none"> - the political context; - legal level; - organizational level; - semantic level; - technical level. <p>UN/CEFACT can cover organizational and semantic levels. Legal and technical are to be elaborated by special agencies, such as UNCITRAL, ISO etc. That is why we just recommend our colleagues what issues should be worked out. Thus, we recommend describing the following types of legal regimes:</p> <ul style="list-style-type: none"> - based on international agreements; - based on commercial agreements and practice; - without special international regulation. <p>Here we recommend UNCITRAL what should be described in respect of the first two regimes.</p> <p><u>Igor Furgel</u>: I find this part quite helpful. When the Recommendation is ready we should forward this part to UNCITRAL.</p> <p><u>Alexander Sazonov</u>: We emphasize that personal data</p>

<p>international legal regime.</p> <p>3) It is recommended to describe domain-constituting mechanisms, similar to item 2), for legal regimes based on commercial agreements and/or common trade practice.</p>	<p>protection issues should be taken into account when establishing a regulating legal regime.</p>
<p>Summary</p>	
	<p><u>Alexander Sazonov</u>: I would like to point out the issues to be elaborated to finalize the draft – it is the Foreword and the section dedicated to communication with organizations on standardization on a technical aspect (ISO, ETSI). Your suggestions are welcome. Also we should discuss attributes of an e-document one more time.</p> <p>I suggest making another conference-call in October before the next UN/CEFACT forum and prepare a final draft for a public review at the Forum. Please feel free to forward any corrections and ideas on our work, I will try to add it to the draft.</p> <p><u>Igor Furgel</u>: Agree.</p> <p><u>Dmitry Iakymenkov</u>: Agree.</p>

All comments will be taken into account in the Recommendation for ensuring legally significant trusted trans-boundary electronic interaction draft version 0.91.