Recommendation for ensuring legally significant trusted transboundary electronic interaction

CONFERENCE CALL

20 February 2015

Attendance

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

General summary – overview

- Members welcome.
- Trust services types concerning
  - It was agreed to consider basic document attributes that are necessary to provide document legal function fulfillment as the basis for trust services types description.
  - It was suggested WG experts to forward information about the document attributes mandatory (and non-mandatory) in their countries and accumulate it one table:

№	Attribute type	Mandatory yes/no	Description/comments
1	…	…	…
…	…	…	…

  - For enabling a legally significant transboundary interchange of electronic documents, there is an opportunity to establish and to use a special type of trust services called 'gateway'. On technological level a gateway shall implement some protocol translation or translation of different protocols or standards from one jurisdiction to another.
  - Trust services (incl. gateways) works with national identification schemes on the one hand and with international trust infrastructure (other trust services) on the other.
  - If there is a gateway between jurisdictions, there should be a profile for this gateway based on agreement between these jurisdictions. Each gateway profile should "know" what attributes are mandatory for each jurisdiction.
- Levels of trust concerning
  - It was agreed to make levels of trust description based on three aspects: legal regime of operation, risk aspect and technological requirements.
  - If trust services engaged in document lifecycle (incl. chain of gateways between the document's issuer and recipient) have different levels of trust the overall level of trust is equal to the weakest of them.

Detailed summary of each agenda item

Recommendation outline points discussed:

<table>
<tr><th>topics</th><th>comments</th></tr>
<tr><td><b>2.4. Trust infrastructures services technical interoperability ensuring approaches</b></td><td></td></tr>
<tr><td>To workout trust services types it is proposed to consider base documents attributes that are necessary to provide document legal function fulfillment.
<table>
<tr><th>№</th><th>Attribute type</th><th>Name of document attributes</th><th>Comments</th></tr>
<tr><td>1.</td><td>Content</td><td>1) document type
2) document classification
3) document title
4) table of contents
5) document body
6) annexes</td><td>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 and authenticity are to be assured when processing, storing and transferring.</td></tr>
<tr><td>2.</td><td>Document issuer legal status</td><td>1) logotype
2) name of a issuer
3) issuer reference data (address, contacts etc.)
4) seal impression</td><td>It can be performed through forming of an authorized body that provides electronic register assuring the attribute validity property.

or

can be fixed with a special attribute in electronic seal certificate.</td></tr>
<tr><td>3.</td><td>Signatory status (powers)</td><td>1) signatory position</td><td>Can be performed trough forming of an electronic register of authorized persons, containing a brief

description of powers with their duration stated.

or

Can be fixed with a special attribute in electronic signature certificate.</td></tr>
<tr><td>4.</td><td>Signature</td><td>1) issuer‘s signature
2) signatur</td><td>Can be performed trough using of an electronic signature (for natural persons) and/or electronic seal (for</td></tr>
</table>
</td><td><u>Dmitry Iakymenkov</u>: The description is good. Still I propose to describe possibility of implementation into negotiations both between different jurisdictions and within one jurisdiction for the cases when we have not only common language, but also common data types. But this is the final step. Now, indeed, we should concentrate on negotiations between different jurisdictions and different types of documents. We should work out common sets of attributes for documents, formats, encryption etc. And the final step is to create a final standard to move to. Jurisdiction can have their national types of documents and formats, and there should be services that convert national formats to the ones of negotiation in transboundary exchange. This service can be a trust service provider but it is to be located in the same jurisdiction as the user.

<u>Aleksandr Sazonov</u>: Agree. To achieve it we need to work out the minimum of attributes and formats that should be implemented into exchange between trust services.

<u>Dmitry Iakymenkov</u>: We can propose xml-based exchange and standards for digital verification of foreign digital signature.

<u>Aleksandr Sazonov</u>: Digital signature is only one of the technologies for purpose of authentication of document. But in practice digital signatures as a PKI solution are not implemented in some countries. There can be national means of authentication other than the PKI-based ones and we can’t compel these countries to use PKI digital signatures. We should adapt national trust services that work with identification schemes on the one hand and with international trust infrastructure on the other. Within this trust infrastructure PKI can be used as a best practice solution.

<u>Andrea Caccia</u>: Standardization activity is related to technologies and digital signature is a legal concept and not an object of standardization. Each country decides which technology use to implement electronic signatures. And we can create some gateway but actually every jurisdiction has a right to decide concerning legal value of a digital signature and other PKI solutions. There will be mutual recognition of systems when there is an agreement between jurisdictions.

<u>Igor Furgel</u>: Agree. It is up to each jurisdiction or jurisdiction domain as the European Union adopted a document on e-signature and this document is not national but for a cluster of countries. On technological level a gateway can be one of the opportunities to implement some protocol transformation or transformation of different protocols or standards from one</td></tr>
</table>

		e stamp of conformation 3) signature stamp of approval 4) visa (clearance / endorsement stamp) 5) copy certification stamp 6) electronic seal of issuing organisation 7) etc.	legal entities). 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.
5.	Date and place	1) date 2) place	Time stamps, attached on the basis of a trusted time source (the validity aspect). Place ##?

jurisdiction to another. A legal basis for it should be an agreement between countries. The question is which part of complex of juristic, organizational and technological aspects can be reflected in the CEFACT Recommendation. We need to cooperate with UNCITRAL, perhaps, in order to synchronize activity on jurisdictional level and standardization organizations such as ISO.
I suggest xml-coding of documents. I also suggest leaving all the technological issues to some annex to the Recommendation as working examples in order to comply with the principle of technological neutrality.

Aleksandr Sazonov: I agree with the idea of neutrality, the xml variant and as to put it to an annex. In the main body we should describe the minimum of document attributes regardless the document format. On the basis of these attributes we can work out types of the services providing verification of these attributes.
Still eIDAS services don’t cover powers of a person.

Dmitry Iakymenkov: We should decide the limits of technological neutrality. For example, in my country an e-signature is a mandatory attribute of an e-document. Different countries have different mandatory attributes.

Aleksandr Sazonov: When trust services work with national users they should use national technologies. And when they deal with other services they should use PKI technologies, for example.

Ramachandran P.: Is it necessary to identify the service providers by a number or another ID?

Aleksandr Sazonov: The matter of mutually recognition of trust services is considered above in the Recommendation.

Igor Furgel: The suggestion is to abstract from a particular technology how an e-signature can be provided. For identification of determination of origin a symmetric cryptography can be used as alternative to PKI. We should put the best practices to an annex.
And there are some basic attributes of documents common for all the countries, such as date. It will be good, if all the participants agree upon minimum of these attributes and we update the table in the draft with this information.

Aleksandr Sazonov: Agree. We should create a table containing set of the attributes necessary for a document to fulfil its legal function. Extra attributes mandatory in some country can be marked as critical for further verification.

Dmitry Iakymenkov: We should provide the same mechanism for reverse procedure as well.

Igor Furgel: If there is a gateway between jurisdictions, there should be a profile for this gateway based on agreement between these jurisdictions. Each gateway profile should “know” what attributes are mandatory for each jurisdiction.

	Bud P. Bruegger: How will it comply with privacy requirements when a document is converted at a gateway? Wouldn't it better if trust services give instructions how to convert a document according to requirements rather than do it themselves? So that they do not see the contents of each document. If a gateway "sees" the contents of business documents it can contradict data protection legislation in some countries. Aleksandr Sazonov: There can be two situations. First. If both parties, who send and receive a document, can agree on a common format and attributes, they can use any transport technology they prefer. And then the receiving party can use some service to verify attributes. Second. If the parties fail to agree upon the attributes, they can use some service which will convert the document from one format to another. In this case there should be strict confidentiality requirements. Bud P. Bruegger: We can use a receipt of translation instead of full translation and instruction of elements corresponding (element X in one jurisdiction corresponds to element Y in another). Igor Furgel: A party can decide not to encrypt metadata or to encrypt part of it. The infrastructure should provide different opportunities depending on agreements between jurisdictions and between communication parties. So the gateway will not inspect the encrypted body, only metadata and convert the document on the basis of metadata. Aleksandr Sazonov: Please forward me information about the document attributes mandatory in your countries. I will include it in this table. Igor Furgel: It will be helpful also to mention non-mandatory attributes in the table. ___: Does the set of documents depend on type of a document? Igor Furgel: Yes, it does. But usually there are attributes common for all types. We should contact UNCITRAL to consult on this issue.
2.5. Trust infrastructures services levels of trust	
It is proposed to consider different possible legal regimes as a basis for trust infrastructures services level of trust description. Possible legal regimes: – Based on international agreements (conventions) and/or on directly applicable international regulation (e.g. trust services that operates in accordance with European Regulation (eIDAS) or EEU Agreement and other documents). – Based on commercial agreements and/or common trade practice (e.g. trust services that operates within LSP such as PEPPOL). – Without special international regulation (e.g. commercial email	Aleksandr Sazonov: I can see three approaches to definition of levels of trust services. The first one is based on the concept of legal regimes. It provides that level of trust service depends on the legal regime it operates in. Thus the high level trust services can operate within international agreements. The medium level trust services work within commercial agreements (LSP such as PEPPOL). The lowest level trust services work within best practices but not governed by agreements or legal basis (e-mail exchange). The second approach we can see in eIDAS regulation. This regulation provides that levels of trust can be regarded on the basis of risk consideration. If one wants to minimize risk, the high level should be used. And when the security requirements are lower, medium or low level of trust can be used. The third approach is based on requirements the trust service meets. If it meets some international requirements, than it is a high level trust service. If it meets requirements set by regulation

<table>
<tr>
<td>services, non-qualified certification authorities, cloud services etc.).
<table>
<tr><th rowspan="2">Requirements conformation</th><th colspan="3">Trust infrastructures services level of trust</th></tr>
<tr><th>basic</th><th>medium</th><th>high
(qualified TSPs)</th></tr>
<tr><td>Meet the requirement laid out in the applicable regulation:
▪ international regulation for centralized TSPs
▪ national regulations for decentralized TSPs</td><td>no</td><td>no</td><td>yes</td></tr>
<tr><td>Meet ICC Compliance criteria</td><td>no</td><td>yes</td><td>yes</td></tr>
<tr><td>Meet the recognized best practices for TSPs</td><td>yes</td><td>yes</td><td>yes</td></tr>
</table>
</td>
<td>other than international, it is medium level. And if meets just best practices, than it is a lowest level trust service.
I think all these approaches can be used.

Dmitry Iakymenkov: Agree. There should be definition of levels of trust on a technical level.

Aleksandr Sazonov: I suggest making a description of all the trust levels. The description should include three aspects: legal regime of operation, risk aspect and technological requirements.

Dmitry Iakymenkov: Agree.

___: Agree. But also it will be reasonable add procedural requirements. We should consider technological and procedural aspects together.

Aleksandr Sazonov: It can be implemented with some common regulation for each type of service and each level of trust. If a trust service operates according to this regulation, it can be considered as a trust service of the corresponding level of trust.

___: Not sure this is helpful, but definition of assurance levels should be considered as a chain to have a source document implemented in a certain technology.

Igor Furgel: During the whole document life, starting with the issue and up to verification in the court, there could be some transformations with the document. At each step of transformation technological and procedural measures will be applied and each of them has certain level of trust. The overall level of trust is equal to the weakest of them.</td>
</tr>
</table>

All comments will be taken into account in the Recommendation for ensuring legally significant trusted trans-boundary electronic interaction draft version 0.7.