Recommendation for ensuring legally significant trusted trans-boundary electronic interaction

draft
version 0.4

Contents

Foreword

Executive summary

1. Recommendation № ___ : Recommendation for ensuring legally significant trusted trans-boundary electronic interaction

1.1. Scope

This Recommendation seeks to encourage the use of electronic data transfer in international trade scenarios by recommending Governments the principles of establishing and operating regional and international coordination organizations for ensuring trust in international exchange of data and electronic documents between participants.

Примечание [s1]: To be discussed one more time during the next conference call.

1.2. Benefits

Harmonized regional and international coordination based on common principles will provide a smooth, transparent and liable environment for electronic activities in trans-boundary trade scenarios. This will make it possible to attach legal significance to an electronic interaction for legal bodies and economic operators regardless of their location and jurisdiction.

1.3. Use of International Standards

The use of international standards can play a key role in larger acceptance of chosen solutions and eventually interoperability. Insofar as possible, legal and private actors who intend to use electronic data transfer in international trade scenarios should try to make use of existing international standards. Technical standards which were able to be identified during the development of this Recommendation are referenced in Annex B.

1.4. Recommendation

The existing natural peculiarities (historical, cultural, political, economic, technical, etc) of different world regions cause also different level of trust within these regions concerning *electronic interaction*.

To Governments and entities engaged in the international trade and movement of goods, providing services and payment processing and willing a tighter, more transparent, effective and easier co-operation concerning *electronic interactions*, the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) recommends establishing and using a dedicated Common Trust Infrastructure (hereinafter CTI).

The primary objective of CTI is ensuring *legally significant electronic interactions* between its users by providing *trust services* of different qualifications (basic, medium, high) to the participants of *electronic interaction.*

The CTI is a fundamental, easily scalable platform providing a unified access to trust services. Herewith, the existing electronic systems are taken into account, so the requirements to their updating for connecting to the CTI are expected to be minimal.

In order to achieve this objective, UN/CEFACT recommends:

- CTI establishment principles;
- CTI coordination approaches;

– approaches ensuring technical interoperability of CTI services;
– levels of trust provided by CTI;
– standardization organizations to co-operate with.

2. Guidelines on how to implement the recommendation

2.1. Terms and Definitions[1]

For the purposes of this document the following terms apply:

Common Trust Infrastructure (CTI)

infrastructure ensuring the *legal significance* of transboundary *electronic interaction*. CTI provides a set of *trust services* harmonised on the legal, organisational and technical / technological levels to its users.

electronic interaction

– a way of *information interaction* based on use of information and communication technologies (ICT). ICT refers to technologies that provide information processing (creation, access, transformation, transmission, destruction, etc.) in the telecommunication context[2].

legal significance (of an action)

– a property of an action (of a process) to originate (to result in) documents (*data unit*) possessing *legal validity*.

legal validity (of a document, or, generally, of data)

– a property of a document (*data unit*) to be applicable for judicature, i.e. be deemed to have satisfied the requirements of applicable law. The *legal validity* is conferred to a document by the legislation in force, by the authority of its issuer and by the established order of its issuing (e.g. it shall be usable for a subsequent reference).

level of qualification (of a service)

– a property of a *service* to evidently fulfil a pre-defined set of requirements on it.

A service may be a *trust service* or an *authentication service* or any other kind of services, to which this term may be applicable.

[1] *Italic face* tags the terms defined in the current Recommendation

[2] ICT is similar to Information Technology (IT), but focuses primarily on communication technologies. This includes the Internet, wireless networks, cell phones, and other communication mediums

There may be different, usually incremental *qualification levels* of a service like ‘zero’, ‘basic’, ‘medium/advanced’, ‘high/qualified’ etc. The lower is the *level of trust* between the participants of *information interaction*, the higher might be demand on the *qualification level* of *services* used by them.

levels of trust **(**between the participants of *information interaction***)**

- a societal function determining the degree of trust between the participants of *information interaction*. Depending on an established or felt level of trust, the participants of *information interaction* are prepared to share a certain amount of resources and to jointly use certain infrastructures.

  For example, with conditionally ‘high’ or ‘medium’ level of mutual trust between the participants, they may be prepared to jointly use centralized international services applied according to the standards agreed upon. In case of conditionally ‘low’ level of trust, the participants may be prepared to use only services built according to the decentralized principle – own services of each participant with a kind of link between them.

trust service

- (high level definition) **-** an electronic service purposing to ensure a certain *level of trust* between the participants of *electronic interaction*.

or

- (lower level definition, will be clarified during Recommendation development) **-**

  1. a service that is reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

  2. trust service is a set of requirements and enforcement mechanisms for parties to authenticate and exchange information

  3. eIDAS definition.

trusted electronic interaction

- the exchange of any data in electronic form in such a way that a user of these data undoubtedly accepts them according to its Operational Policy. It is a matter of a concrete Operational Policy, which way is considered as a *trusted* one. Hence, the determination of the trustworthy of some data varies from one concrete case to another. Trusted electronic interaction is provided by using *trust services*.

2.2. Common Trust Infrastructure establishment principles

- **Scalability**. The CTI is established in such a way that it can be easily scaled. It broadens easily at any level of consideration due to the accession of new participants, such as new jurisdictions, new supranational participants, new operators of trust services, and register systems.

- **Traceability**. Any fact of electronic data exchange within the CTI should be fixed and available for conflict resolutions if necessary.
- **Cost efficiency**. While the CTI architecture variants comparison the risk analysis should be taken into account.
- **Complexity**. Coherent elaboration of legal, organizational and technological issues should be done within CTI establishment. A complex description allows correct functioning of the system as a whole and its single elements.
- ...##

Примечание [s2]: Can be added later

2.3. Common Trust Infrastructures coordination approaches

Identify the principles of establishing and operating regional and international coordination organizations for ensuring trust in infrastructures that satisfy organizational and administrative regulation of legally significant trans boundary electronic data exchange

Identify the underlying principles and content for Model MoUs/Agreements between two or more countries regarding Mutual Recognition of Digital and Electronic Signature Certificates

Примечание [s3]: From the project proposal

There are three levels of coordination: legal, organizational and technological.

Legal level

The CTI can be built on a single- or multi-domain basis. In the context of legal and organizational regulation, the multi-domain basis is the most complicated variant. Fig. 1 gives a general scheme of a legal regulation.

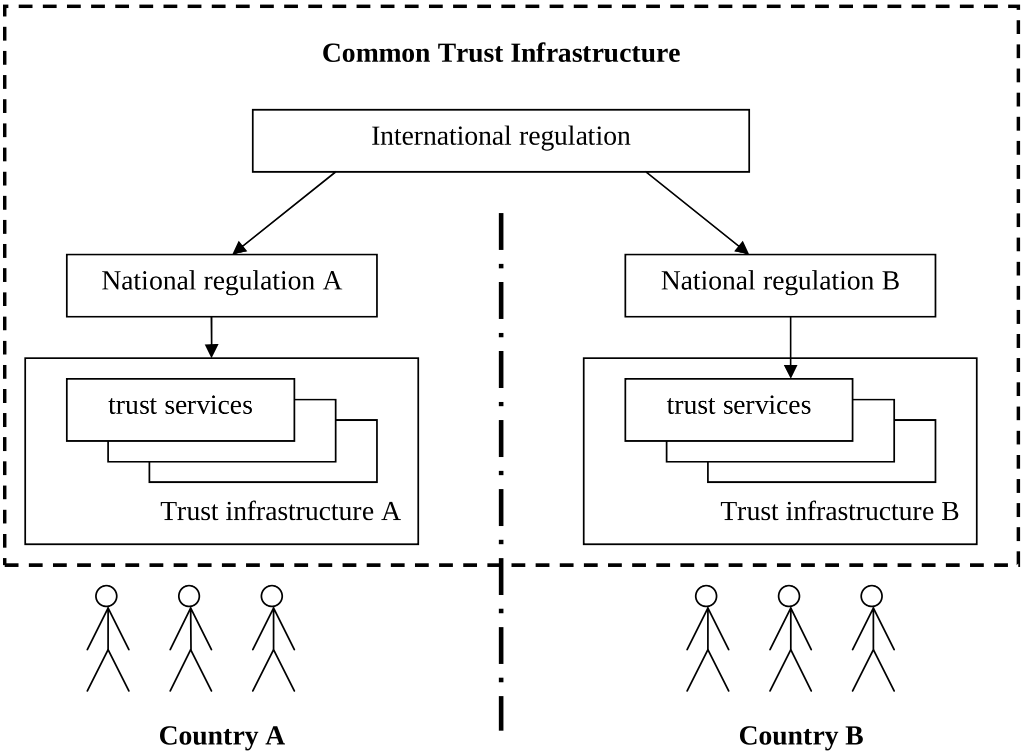

Fig.1. Legal level

Legal regulation of CTI interaction can be divided in two parts: international and national. The international legal regulation is carried out on the basis of the following types of documents:

– international treaties/agreements;
– acts of different international organizations;
– international standards and regulations;
– agreements between participants of transboundary information interaction on given issues;
– model acts.

The national legal regulation is built on a complex of normative documents that are standard in each particular jurisdiction.

We recommend a tight cooperation with UNCITRAL in order to harmonize the effort of this Recommendation concerning the necessary coordination on the legal level, see sec. 2.6.

Organizational level

Mutual legally significant recognition of trust services provided under jurisdiction of various states is reached through creation and operation of the dedicated body (let call it International Coordination Council or ICC) that includes national regulation bodies. The activity of ICC is regulated by the ICC Statute which is to be recognized and signed by all its authorized members – that is the Regulation Bodies of the Electronic Data Interchange represented primarily by the National Regulators of the CTI.

Technological level

There can be a great number of technological options for trust services' realization. The main requirement to the CTI elements is interoperability. Regulation at this level is carried out with application of different standards and instructions set forth by the ICC documents.

2.4. Trust infrastructures services technical interoperability ensuring approaches

Identify approaches to ensuring interoperability of technical systems, infrastructures of trans boundary electronic data exchange and end users including functional requirements and information security requirements.

Identify appropriate trust services types provided by the trusted infrastructures for ensuring legally significant trans boundary electronic data exchange.

Примечание [s4]: From project proposal

2.5. Trust infrastructures services levels of trust

Identify the possible levels of trust afforded by the trusted infrastructures and mechanisms by which these levels can be provided. For example, lower levels of trust may not require government directives for achieving a legally significant electronic interaction. UN/CEFACT recognizes that guidance for required levels (possibly higher) of trust and for desired levels of authentication depends on specific circumstances but such guidance does not constitute the scope of this recommendation. For these different levels of trust identify:

- common set of requirements trust services must comply with. Such requirements are to cover the following aspects: security, accessibility, and interoperability

- best practices for trust services initiation, certification and audit procedures.

Примечание [s5]: From project proposal

2.6. Communication with organizations in different areas of standardization

Identification of international organizations in different areas of normative and legal regulation and policies (such as WTO, UNCITRAL, WCO and others) for participation in the defining conditions for establishing necessary level of trust between the participants of the trusted infrastructure that will ensure legal significance of transboundary electronic exchange of data issued in different jurisdictions.

Identification of international organizations in different areas of standardization (such as ISO, W3C, ETSI and others) for participation in all the technical aspects of forming and functioning transboundary trust space.

Примечание [s6]: From project proposal

3. ANNEX 1

Terms and Definitions[3]

authentication

– Anders Tornqvist: means an electronic process that allows the **confirmation** of the electronic identification of a natural or legal person; or of the origin and integrity of an electronic data.

Примечание [AN7]: I agree.

– Igor Furgel: a process of the verification of *authenticity*. A successful *authentication* (along with other factors) can be a necessary condition for the determination of the *legal validity* (of an *entity*).

– Eric E Cohen (http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf):

Код поля изменен

1. The act of verifying identity (i.e., user, system)
Scope Note: Risk: Can also refer to the verification of the correctness of a piece of data

2. The act of verifying the identity of a user and the user's eligibility to access computerized information
Scope Note: Assurance: Authentication is designed to protect against fraudulent logon activity. It can also refer to the verification of the correctness of a piece of data.

Примечание [IF8]: This is ‚**authorization**', but not ‚authentication', see below

– Ramachandran: the process of validating the identity of someone or something. Generally authentication requires the presentation of credentials or items of value to really prove the claim of who you are. The items of value or credential are based on several unique factors that show something you know, something you have, or something you are.

A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit.

authenticity

Примечание [AN9]: –Cf the VAT Directive 2010/45 where in relation to the "authenticity" of an invoice the following is commented: "The supplier must be able to provide assurance that the invoice was indeed issued by him or in his name and on his behalf." –

– Anders Tornqvist: means that the **data** can be checked for its authenticity in a certain context.

Примечание [IF10]: ‚authenticity' is defined by using ‚authenticity'; it is a dead loop.

– Igor Furgel: the property of an entity to evidence the identity of its issuer.

– Ramachandran:

1. The *authenticity* is an auditable process that ensures a high level of quality in the results by maintaining evidence of trustworthiness of the identity and integrity of data messages
2. *Authenticity* is the status of being dependable in regard to evidence of identity and integrity in accordance with the agreed level of assurance.

[3] *Italic face* tags the terms defined in the current Recommendation

3. *Authenticity* is generally understood in law to refer to the genuineness of a document or record, that is, that the document is the “original” support of the information it contains, in the form it was recorded and without any alteration.” Authenticity is the property of being genuine and able to be verified and trusted.
4. *Authenticity* in the electronic environment, further to the high levels of identification, evidentiary and attribution functions may be able to be established through an “authentication framework.” This “authentication framework” would involve legal infrastructure, some technical infrastructure and some organizational infrastructure.

***authorization** (as a process)*

– Eric E Cohen: the approval, permission, or empowerment for someone or something to do something.

Примечание [s11]: Eric E Cohen This is in contrast to when you care not whether the agent is authorized, only that they are who they say they are - authentication. The two are usually considered orthogonal; you normally only wish to check one or the other. I believe in transboundary efforts, authorization is more important than authentication.

– Igor Furgel: approving a subject (a person, an IT component or a process acting on behalf of them) for the execution of a certain action.

certificate

– Jari Salo (http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf):

Код поля изменен

means a data message or other record confirming the link between a *signatory* and signature creation data.

data unit

a set of digits or characters treated as a whole.

digital certificate

– Aleksandr Sazonov: means a data message or other record confirming the link between a public key (validation data) to a particular distinguished name in the X.500 tradition.

– Igor Furgel: means an electronic attestation which links signature validation data of an entity to the entity and confirms the identity of that entity.

digital signature

– Eric E Cohen (http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf):

Код поля изменен

A piece of information, a digitized form of signature, that provides sender authenticity, message integrity and non-repudiation.

A digital signature is generated using the sender’s private key or applying a one-way hash function.

– Igor Furgel (ISO 7498-2 (1989): ‘Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture’):

Data appended to, or a cryptographic transformation of, a *data unit* that allows a recipient of the *data unit* to prove the source and integrity of the *data unit* and protect against forgery, e.g. by the recipient.

– Ramachandran: a *digital signature* is made when the owner of a key pair uses its private key to "sign" a message. This signature can only be verified by the corresponding key.

electronic signature

– Anders Tornqvist & DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures: means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

Примечание [IF12]: This definition is not a full one, there are also other services of electronic signature.
The main services of a signature are (i) perpetuation function (a signature can be verified by anybody later on at any time), (ii) the determinability of the identity of signatory. Additionally, there are warning and consciousness functions.

– Eric E Cohen (http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf):

Код поля изменен

Any technique designed to provide the electronic equivalent of a handwritten signature to demonstrate the origin and integrity of specific data.

Digital signatures are an example of electronic signatures.

Примечание [IF13]: There is a quite controversial discussion on it.

– Igor Furgel:

data in electronic form which are attached to or logically associated with other electronic data. *Electronic signature* documents a relationship between the *signatory* and these other electronic data and enables (also) a third party to subsequently ascertain this relationship.

– Jari Salo (http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf):

Код поля изменен

data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.

Примечание [IF14]: Not unconditionally an approval, but, generally, a relationship between the signatory and the message

Примечание [AN15]: The UNCITRAL definition is not uncontroversial. We should also look at the new definitions of e-signature and e-seal of the EU EIDAS Regulation, rather than the -99 Directive referenced above.

– Ramachandran: Data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's intention in respect of the information contained in the data message. An electronic signature should not be discriminated because of its origin. But may be discriminated because of their intrinsic qualities

entity

– Igor Furgel: can be a document, a record, an identifier etc (generally: a *data unit*).

genuineness (in IT)

– Igor Furgel: *integrity* + *authenticity* = the property of an *entity* to evidence:

(a) not having been altered from that created by its issuer
AND
(b) the identity of its issuer.

– Ramachandran: the quality that ensure document's property of being genuine.

genuineness (in law)

Примечание [IF16]: The foot note No. 5 in the REC. 14 may also be helpful here:
"In general, signature and authentication in an Information Technology (IT) environment often encompass some inherent functions which can vary from integrity, genuineness, proof, security, etc. Again, all of these terms can have differing interpretation based on environment and geography. This Recommendation has been prepared to align itself with the works of UNCITRAL while remaining consistent with the use of these terms in other UNECE trade recommendations. When reading or drafting any text on the subject, clear identification of which approach is being used, is recommended. For legislators who will probably use a legal definition, reference to UNCITRAL documents on the subject is recommended in order to clearly identify the legal use of these terms. "

– Igor Furgel: (130201+Rec14+survey+on+def_levels+consolidated+responses): "*Authenticity* is generally understood in law to refer to the *genuineness* of a document or record, that is, that the document is the "original" support of the information it contains, in the form it was recorded and without any alteration.” *Authenticity* is the property of being *genuine* and *able to be verified and trusted*".

‘*Genuineness’* in law is equivalent to ‘*authenticity*’.

information interaction

– Igor Furgel: the interchange of any data between the participants of interaction

integrity

– Igor Furgel: the property of an *entity* to evidence **not having been altered from that created by its issuer**.

– Eric E Cohen (http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf):

Код поля изменен

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Примечание [AN17]: Perhaps not always “guarding against” but rather allowing for detection of change.

– Ramachandran:

1. *DATA INTEGRITY*—A condition in which data has not been altered or destroyed in an unauthorized manner
2. *Integrity* is a state of information that assure that it is accurate,complete, consistent and has been protected from errors or unauthorized modification.
3. *integrity* refers to the resource is untampered with, uncorrupted and complete in all its essential respects after the act of signature is carried out.

levels of access

– Igor Furgel: permission for a subject (a person, an IT component or a process acting on behalf of them) to get a specified kind of access (e.g. write, read, etc.) to specified objects (e.g. data, processes, information, other resources).

A successful *authentication* (along with other factors) can be a necessary condition for granting a certain *access level*. The terms ‘access level’ and ‘authorization level’ are used as synonyms in the context of the current Recommendation.

levels of authentication

– Aleksandr Sazonov: a synonym for *levels of qualification of authentication service.*

– Ramachandran: a guidance concerning control technologies, processes, and management activities, as well as assurance criteria that should be used to mitigate authentication threats in order to achieve the required level of security based on the sensitivity of data or a service.

non-repudiation

– Eric E Cohen: the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified. A user cannot deny/repudiate that they signed/sent a message.

privacy

Примечание [AN18]: Should we deal with “privacy” or “personal data” rather?

– Eric E Cohen (http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf):

Код поля изменен

Freedom from unauthorized intrusion or disclosure of information about an individual and an organization.

Примечание [s19]: Eric E Cohen My *personal* interpretation includes information about both individuals (people) *and* organizations.

signatory

– Jari Salo (http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf):

Код поля изменен

a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents.

Примечание [IF20]: Not just acts, but creates an electronic signature

Примечание [AN21]: Possibly only “creates”, not necessarily ”acts on behalf”.

– Igor Furgel (Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions):

a natural person who creates an *electronic signature*.

time stamp

Удалено: ***stamping***

– Eric E Cohen: a trusted indication of when an action, particularly the application of a digital signature, took place.

Примечание [s22]: Eric E Cohen Time stamping is vital in cryptography as people change roles and signatures expire; it is important to know whether the signature was valid and the signer was authorized or could be authenticated at the point of *signing* rather than the point of *checking*.

– Igor Furgel (Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions):

data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

transboundary trust space

– Aleksandr Sazonov: a set of normative, organizational and technical conditions for establishing trust in transboundary electronic interaction between public governmental authorities, public non-budgetary funds, local authorities, organizations and citizens.

– Ramachandran: a technological and legal framework for trust establishment in transboundary electronic informational interaction of entities in different legal frameworks’ subjects.

– Eurasian Economic Community Agreement: 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.

trust domain

– Igor Furgel: informational and legal space using the same CTI

what-you-see-is-what-you-sign

– Aleksandr Sazonov: is a desirable property of electronic signature systems meaning that the semantic interpretation of a electronically signed message cannot be changed, either by accident or by intent.

XML Signature