Mutual recognition mechanism of legally significant e-documents and data in cross-border document flow

V N Kustov¹ and E S Silanteva²

¹ Informatics and Information Security Department, St. Petersburg state Railways University of Emperor Alexander I, 9 Moskovsky Ave., Saint Petersburg, North-Western Federal district, 190031, Russia
² LLC "NST", 107078, Moscow, Orlikov lane, house 5, building 2, floor 09, room 34, Russia

E-mail: kvnvika@mail.ru, ceo@newspaceoftrade.com

Abstract. In this article we will observe mutual recognition mechanism that can provide transparent and reliable environment for data and documents in electronic form exchange across borders. Implementation of the Mutual recognition mechanism concept will help to facilitate interaction and ensure trust between parties taking part in cross-border legally significant e-documents exchange.

Mutual recognition mechanism is a set of legal, organizational, semantic and technical conditions for reciprocal recognition of the validity of data and documents in electronic form exchanged across borders among two or more countries. Mutual recognition mechanism allows public authorities, physical and legal entities to interact in the framework of relations arising during generation, sending, transmission, reception, storage and use of legally significant data and documents in electronic form exchange across borders. Cross-border exchange of legally significant data and documents in electronic form between countries can be exercised by the trust ensured by the Trust services providers. Trust in paperless transboundary interaction is a set of objective signs that are used in electronic interaction. For example, electronic signatures are recognized as electronic signatures and their signed electronic documents are validated as documents signed by subjects of legal relations (owners of electronic signatures), the identity of which is confirmed. In this article we will observe Transboundary trust environment (TTE). TTE is a set of normative and organizational-technical conditions which implementation provides the mode of trust in electronic interaction with the participation of a limited or unlimited number of members. TTE as an integral structure operates based on a set of trusted services and may include a trusted third party. Trusted Third Party (TTP) is the organization responsible for the relevant trust that should be provided to complex information technologies and organizational-legal measures to ensure legally significant electronic interaction. Also, the article describes conceptual model of the mutual recognition mechanism.
1. Introduction

1.1. Relevance of the issue

Technological innovations are increasingly used to facilitate the exchange of documents between various parties domestically and abroad. Business and government invest in Single Window [1] and other paperless systems. IoT, Big Data, Wireless, etc. transform the world. This process is called «digital conversion». But implementation of these tools should be used to achieve some goal. Kupriyanovskiy V, Namiot D and Sinyagov S. name better economy as this goal [2]. Modern world turns to the creation of the cyber-physical (CPS) systems that connect physical production processes with software-electronic systems [3]. These systems, by volume of processed data, related to the Big Data [4]. Moreover, CPS systems have become the reason for the rapid growth of interest in processing large amounts of real-time data. This is an obvious trend in the field of Big Data [5]. So, the goal of modern digital transformation should be named not economy but data economy. The issue is that to build data economy we crucially need to use appropriate data. Trusted data. But from what sources can we get it? Authors consider legally significant data and e-documents as one of these sources. PKI infrastructure provides us with the opportunity to create transboundary trust environment – environment of trusted data. These data could be trusted despite the fact that it was got from different countries with different PKI infrastructures and different legislations. Mutual recognition mechanism is the tool to validate data and e-documents in transboundary trust environment.

1.2. Current status

PKI-based e-signature is widely used to ensure legal significance of e-documents in all areas of relations among business, government and citizens. PKI infrastructure is different in different countries, but the overall picture is exactly the same. Digital economy programs that are being implemented in a number of countries are increasing attention to PKI technologies.

A number of countries have their own cryptographic schools that ensure their digital sovereignty. To provide compatibility at the cryptographic algorithm level, you must either import/export cryptographic tools or create solutions that allow compatibility of various cryptographic tools. Ways of establishing trust relationships between certification authorities of different countries are impossible in the general case, because of the incompatibility of cryptography.

Therefore, we have developed a conceptual model of the Mutual recognition mechanism (MRM) of data and electronic documents exchanged across borders. MRM technically based on trusted third party (TTP) is used to establish trust relationships between PKI infrastructures of different countries, allowing to take into account both the incompatibility of cryptography and the difference in regulatory in various countries, the so-called «different certificates policy».

2. Essence of the Mutual recognition mechanism

First of all, let us explain what Mutual recognition mechanism is. It is a set of legal, organizational, semantic and technical conditions for reciprocal recognition of the validity of data and documents in electronic form exchanged across borders between two or more countries. Subjects of cross-border electronic cooperation in paperless trade are public authorities, physical and legal entities, interacting in the framework of relations arising during generation, sending, transmission, reception, storage and use of legally significant data and documents in electronic form exchanged across borders.

Second, we should mention that this exchange could be exercised by the trust ensured by the trust services providers. Trust service is a hardware and software system, which functioning is provided by the operator assigned in the prescribed manner. Trust in paperless transboundary interaction is a set of objective signs that are used in electronic interaction. For example, electronic signatures are recognized as electronic signatures and their signed electronic documents are validated as documents signed by subjects of legal relations (owners of electronic signatures), the identity of which is confirmed.
Finally, in this way Transboundary trust environment (TTE) is a set of normative and organizational-technical conditions which implementation provides the mode of trust in electronic interaction with the participation of a limited or unlimited number of members. TTE as an integral structure operates based on a set of trusted services and may include a trusted third party. [6] Trusted Third Party (further – TTP) is the organization responsible for the legally significant electronic interaction, ensuring the trust mode of the TTE.

3. Conceptual model of the mutual recognition mechanism

Conceptual model of the mutual recognition mechanism promotes the idea of mutual recognition (MR) by design. This means that Mutual recognition mechanism (MRM) conceptual model is applicable to all digital trust services and national legislations, implementation of this model at national level assists public authorities and business entities with development of the transparent and smooth cross-border exchange of legally significant data and e-documents. Conceptual model of the Mutual recognition mechanism is presented at the figure 1.

![Conceptual model of the Mutual recognition mechanism](image)

**Figure 1.** Conceptual model of the Mutual recognition mechanism.

Conceptual model of the mutual recognition mechanism includes principles of the Mutual recognition mechanism, mutual recognition governance, cross-cutting component institutional arrangement of MR, and four layers of the mutual recognition: legal, organizational, technological and semantic. Let us to describe the components of the model in more detail.

3.1. Institutional arrangement of the MRM

Compliance of the subjects of electronic interaction to the relevant legal, organizational, semantic and technical requirements and/or recommendations, and regulations and/or procedures is provided by the institutional arrangement that ensures observance of the rights and legitimate interests of subjects of electronic interaction.

Institutional arrangement of the Mutual recognition mechanism is the structural component providing interaction among various actors in the paperless documentation with the purpose of data
and documents in electronic form validation. It consists of a set of organizational and technological documents for each trust service. Development and approval of these documents should be the authority of TTE. Institutional arrangement can include following documents: technical requirements for the SHC of trust service; regulations for the operator of the trust service and its authorized persons; rules for clients’ connection with the use of trust service; procedures for issuance and use of access equipment; TSP audit regulations.

It should be mentioned that the purpose of TSP audits is obtaining or maintaining accreditation. Conformity assessment criteria can rely on already existing standards, such as ETSI TS 102 042 [7], Web Trust [8] and others. The accreditation procedure should be held by the responsible Regulator (national or international). Carrying out of a such audit requires special independent infrastructure which main goal is creation of the conditions for holding audit at least on a certain level of quality (volume, depth, and thoroughness). Results of the audits in different countries should be comparable with each other. This «comparability» is a necessary component to achieve the necessary level of trust among participants of the TTE.

3.2. Principles of the MRM
Authors have defined the core principles for Mutual recognition mechanism. They are presented at the table 1. Authors consider implementation of these principles in mutual recognition scheme as the base to create the general levels of credibility and increase operational compatibility.

Table 1. Principles of the Mutual recognition mechanism.

| Name of the principle               | Description                                                                 |
|------------------------------------|-----------------------------------------------------------------------------|
| Client-friendly architecture       | Client-friendly architecture should allow to interconnect systems and services in user-friendly way |
| Cooperation                        | MRM should be based on cooperation between the state and private sectors; |
| Development of infrastructure      | Development of infrastructure of electronic information documenting should run continuously with necessary upgrades. |
| Ensuring of trust                  | MRM should ensure the trust and validity to electronic documents.            |
| Functional equivalence             | It is necessary to analyze functions of the requirements concerning paper documents to define how these functions can be performed by electronic means; |
| Operational compatibility          | Operational compatibility assumes technical and technological compatibility of information systems, including a possibility of data exchange in the all-used electronic formats, and also stability of functioning. Operational compatible systems should have an opportunity to connect the new participants that are located in the country or abroad, allowing them to start to use the system quickly |
| **Reliability of infrastructure** | Reliability of infrastructure assumes application of the general requirements in the field of ensuring reliability of functioning to all participants |
| **Sovereignty** | MRM should guarantee both the possibility of national approaches in formation of National trust environment (NTE) and the recognition (or maintaining unaltered) of the national identification schemes (infrastructures) |
| **Technological neutrality** | Users and applications on different networks should have the opportunity to communicate across different technologies, systems and languages; |

### 3.3. MRM governance
MRM management is a solution that uses mutual recognition, policies, institutional mechanisms, and other various aspects of monitoring and ensuring mutual recognition at the international and national levels. There is a need to ensure the holistic management of mutual recognition activities at all administrative levels and in various sectors of different countries. MRM governance is the key to a comprehensive approach to mutual recognition, since it combines all the tools necessary for its application and allows to manage the legal, organizational, technological and semantic layers.

### 3.4. Legal layer of the MRM
Legal layer of the MRM ensures that organizations operating under different legal frameworks are able to work together. MRM demands clear agreements on how to deal with differences in legislation across borders, including the option of new legislation development. Coherence of the legislation, in view of ensuring mutual recognition, should be assessed before its adoption and through evaluation of its performance regularly once it is put into application. Proposed legislation should undergo a «digital check» to ensure that it provides trust and doesn’t lead to any barriers in digital exchange. Legislation should be developed both at national and international levels. There are several initiatives that are developed all over the world. For example, we can mention that UNCITRAL has developed the Model Law on Electronic Commerce [9] and the Model Law on Electronic Signatures [10] to provide national legislators with a set of internationally recognized rules aimed at elimination of the legal obstacles and increase of the legal predictability in the e-commerce. Also, we should mention the Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific [11] developed by UN ESCAP. It is Asia-Pacific initiative aimed to enhance regional cooperation in cross-border paperless trade.

### 3.5. Organizational layer of the MRM
Organizational layer of the MRM based on documenting and integrating or aligning business processes to exchange of data and documents in electronic form across borders. Aim of this layer at national level is to meet requirements of the international community by making trust services available, easily identifiable, accessible and user-focused. For various commercial and administrative organizations, it may be necessary to coordinate their business processes, redefine them, or re-create them in order to provide trust services efficiently and effectively. Coordination of existing business processes requires their consistent documentation with extensive use of process modeling, taking into account the exchange of necessary information, in order to contribute to the MRM its share in ensuring trust.
At the organizational layer, trust service considered as a tool including means of documents identification and rules for use of trust service. In addition, customers should be provided with judicial, insurance, notarial, archival and other institutional support developed in the traditional paper workflow.

3.6. Technical layer of the MRM
This layer defines the infrastructure and applications, systems and services that are interconnected. Mutual technological recognition involves the development of interfaces and their specification, communication and data exchange services, the creation of a common database, and the development of secure data transfer protocols that allow the secure and confidential exchange of documents and data in electronic form across borders.

From technical point of view Mutual recognition mechanism is a way of establishment of the trust relations between users from different domains of trust.

Each Trust service can be presented as a complex that includes technical and organizational components, staff and users. Thus, each service can be conventionally represented as a set of following components: software and hardware (server equipment and workstations, system-wide and specialized software, data protection, data storage systems, and other specialized components, depending on the type of proxy service). For convenience, we name all of these components as software and hardware complex (SHC): channels (telecommunication equipment and means of access to networks and data transfer channels); managing and operating staff; organizational and administrative documentation; operational documentation; users.

Requirements to information security should be provided to all architectural elements of the TTE, based on the model of information security threats, i.e. formalized presentation of the properties or characteristics of the actual information security threats.

TTP description was provided in ITU-T Recommendation X.842 «Information technology – Security techniques – Guidelines for the use and management of Trusted third party services» [12]. In this document, a trusted third party (TTP) is defined as a separate entity or its representative that provides trust services and is trusted for other entities to which these trust services are provided. The same document contains the most general description of architecture of TTP services interaction from different PKI domains.

One of the possible implementations of the TTP model is Data Validation and Certification Server (DVCS) in accordance with the recommendations RFC 3029 «Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols» that can be used as one component in building reliable non-repudiation services [13]. DVCS receipt allows to provide trust between different PKI domains in case when their cross-certification technically or legally is impossible. For correlation of the certificates policy the receipt of DVCS service can map the policy at the same manner as it is mapped in the procedures of cross-certification. In extension of policy mapping, the intermediate Certification Authority guarantees to the user of the certificate that it will fulfil general guarantees and obligations, even despite the fact that the other users of certification chain work in the other policy area.

Certification Authority (CA) of the integration segment should include one or several mappings for each set of the policies according to which it has issued TTP certificates. This CA shouldn’t include mappings for other policies. Thus, the set of certification authority of an integration segment and the TTP services using certificates of this CA fulfil TTE role between domains with the various levels of reliability. This scheme is presented in the figure 2.
If one or several Certificate policies, in accordance to which Sender of Certification authority acts, is identical to those, in accordance to which Certification Authority of TTP integration segment acts, these identifiers should be excluded from the extension of policy mapping, but included to extension of certificate policies. Policy mapping has effect of transformation of all policy identifiers in the certificates of sender domain to identifier of equivalent policy recognized by the user of certificate (recipient). In this schema identifier of equivalent policy is described in the receipt of TTP service.

In this article we would like to illustrate MRM by a real pilot project. A bridge of trust was built between the Russian Federation and Azerbaijan. In this case Digital trade hub (DTH) provides trust mode to the electronic interaction between two countries. The scheme is presented in the figure 3.

3.7. Semantic layer of the MRM
The semantic layer of mutual recognition is designed to ensure that the exact meaning of exchanged electronic documents and data is preserved, and that they are correctly understood and confirmed throughout the entire cycle of mutual exchange between the parties. The semantic layer works with data values and their relationships. It can include creating semantic dictionaries and various structures for describing and sharing data, and provides the same and accurate understanding of data by all participants in the interaction.

4. Conclusion
The article discusses issues of the Mutual recognition mechanism based on PKI technologies for the legally significant e-documents exchange across borders. Authors proposed conceptual model for development of the mutual recognition mechanism. It covers: principles of the Mutual recognition mechanism, mutual recognition governance, institutional arrangement of the MRM, and four layers of the mutual recognition: legal, organizational, technological and semantic.
Mutual recognition based on common principles will provide a smooth, transparent and reliable environment for data and documents in electronic form exchange across borders. Implementation of the Mutual recognition mechanism will help to facilitate interaction and ensure trust between parties taking part in electronic documents exchange.

![Figure 3. MRM between Russia and Azerbaijan.](image)

Given the different technical legal and administrative environments in different countries Mutual recognition poses significant challenges that can be overcome due to the creation of the trust that will ensure cross-border exchange of data and documents in electronic form among countries. This trust is created in the transboundary trust environment (TTE) by Trusted third party. MRM allows to provide validation of electronic information exchanged across countries when PKIs use different, incompatible.

**References**

[1] UNECE Recommendation 33 2004
   https://www.unece.org/fileadmin/DAM/cefact/recommendations/rec33/rec33_trd352e.pdf

[2] Kupriyanovsky V, Namiot D and Sinyagov S 2016 Cyber-physical systems as a base for digital economy *International Journal of Open Information Technologies* Vol 4 No 2 (MSU Faculty of Computational Mathematics and Cybernetics Russia, Moscow) 18-25

[3] Wolf W 2009 Cyber-physical systems *Computer* 3 88-89

[4] Lee J Lapira E Bagheri B and Hung-anKao 2013 Recent advances and trends in predictive manufacturing systems in big data environment *Manufacturing Letters* Vol 1 No 1 Society of Manufacturing Engineers (SME) (Elsevier) 38-41

[5] Namiot D 2015 On Big Data Stream Processing International Journal of Open Information Technologies 3 48-51

[6] Methodology of formation of transboundary trust environment and the requirements for its creation, functioning and development 2017
   https://www.unescap.org/resources/methodology-formation-transboundary-trust-environment-and-requirements-its-creation-0/
[7] Software Electronic Signatures and Infrastructures (ESI) Policy requirements for certification authorities issuing public key certificates 2013  
https://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf

[8] Web Trust Principles and criteria 2015 https://cabforum.org/webtrust-for-cas/

[9] UNCITRAL 1996 Model Law on Electronic Commerce Electronic resource access mode  
https://unctital.un.org/en/texts/eCommerce/modellaw/electronic_commerce/

[10] UNCITRAL 2001 Model Law on Electronic Signatures  
https://unctital.un.org/en/texts/eCommerce/modellaw/electronic_signatures/

[11] UN ESCAP 2016 Framework Agreement on Facilitation of Cross-border Paperless Trade in Asia and the Pacific  
https://treaties.un.org/doc/sources/docs/ESCAP_RES_72_4-E.pdf

[12] ITU-T 2002 Recommendation X.842 information technology security techniques guidelines for the use and management of trusted third party services. (Geneva) 32  
https://www.itu.int/rec/T-REC-X.842

[13] Network Working Group 2013 Request for Comments 6960 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP  
https://tools.ietf.org/html/rfc6960