The Development of a Structural Scheme of National Segment in a Protected Cross-Border Space

Rustem Biyashev, Saule Nyssanbayeva and Yenlik Begimbayeva*
Information Security laboratory, Institute of information and computational technologies of SC MES RK, Almaty, Kazakhstan
*Corresponding author

***Abstract*—A structural scheme of national segment in a protected cross-border space is proposed. Information exchange in the integrated system of cross-border space between interacting sides is provided by the creation and use of national segment and an integration gateway. The scheme of interaction of two sides of the integration system using the integration gateway is presented.**

Keywords-information interaction; cross-border exchange; space of trust; information security; digital signature

I. INTRODUCTION

An important parameter for the full functioning of the state, especially in the inter-state cooperation is the information security ensuring. According to this the need to create and provide a clear and secure cross-border information interaction of electronic documents and ensuring the legal significance of these documents is also appeared. The relevance of the development of the model of protected cross-border information exchange is due to the fact above.

Cross-border interaction is the interaction of subjects of different legal fields. In such interactions, the following problems occur:

- the unresolved complex of organizational, technological and legal issues of the legal significance of electronic information;

- the development of an effective and reliable rights management mechanism of subjects and provide each side of this interaction own information security and protection of their informational independence.

Electronic cross-border interaction involves collaboration with many disparate information systems. Rights management mechanisms is based on different principles and implemented in different ways in each of these systems [1].

The concept [2] stated that the solution of problems of reliable and effective integration of geographically distributed state information resources and information systems of the member countries, ensuring interaction of authorities of the Member States in electronic form, including opportunities of legally valid electronic documents exchange are the one of key directions of work on the creation and implementation of integrated information system of the Eurasian Economic Union (EAEU or EEU). To solve the problems of providing cross-border information interaction (CBII) is necessary to construct the integrated system.

II. INFORMATION EXCHANGE IN THE INTEGRATED SYSTEM OF A CROSS-BORDER SPACE

Information exchange in the integrated system of cross-border space (hereinafter referred to as Integrated System) between interacting sides is provided by the creation and use of the national segment (hereinafter referred to as segment) and an integration gateway (hereinafter referred to as gateway). These segments are a set of secure system of data transmission, included to each interaction side's node in information exchange.

In the CBII in the transmission and receipt of electronic documents is required to verify these documents with digital signature, which confirms its legal value or validity. The legal significance of the document in the integrated system is confirmed on the basis of trusted third party (TTP) services.

Guaranteed trust of TTP services is based on the guarantees that electronic documents are available only to the required recipient with the time fixing and with the ensuring the integrity, authenticity, authorship and privacy. Also appropriate procedures of the providing of the necessary evidence is carried out which legally binding and allowed to restore the sequence of events in the processing and conversion of electronic documents [3].

At the documents circulation in the cross-border space of trust are arising conflict situations. These situations are connected with formation, delivery, receipt and receipt confirmation of the electronic document, and also with the use digital signature (DS) in documents. Resolution of conflict situations is included to the tasks of specialized operator. The certification authority (CA) is the specialized operator in the integrated system. Conflict situations in system are arising in the following cases:

- failure to prove of the authenticity of protected electronic documents by means of DS verification of recipient;

- contesting the fact of identification of the owner of DS which signed the electronic document;

- the statement of sender or recipient of the electronic document on its distortion;

- contesting the fact of sending and (or) receipt of the protected electronic document;

- contesting time of sending and (or) receipt of the protected electronic document;

- other cases of conflict situations.

TTP infrastructure and certification authority is located in national segments and organized at the level of each interacting sides.

III. Development of Structural Scheme of Segment in the Integrated System

In the implementation of the structural scheme of the protected CBII are applied the basic terms and definitions of model law "On the cross-border information exchange of electronic documents" [4].

In this paper, model of structural scheme of interaction between two sides in the integrated system are proposed. Structural scheme of interaction of sides "A" and "B" of the cross-border information exchange is shown in Fig. 1. The modeled technology on the example of information transmission from side "A" subscribers to side "B" subscribers is considered.

Information interaction between sides "A" and "B" in the exchange of confidential electronic documents is proposed to implement using a special automated system CBII - Integration Gateway.

Integration Gateway consists of two or more automated workstations, depending on the number of cooperating sides. Each automated workstation is the property of one of the interacting sides and protected by accepted protection means of appropriate sides. Cryptographic and hardware and software information security means from unauthorized access, and other hardware and software are determined for workstations of each interacting sides. Information is transmitted over a secure channel. In the information transmission over such channel using the integration gateway, the implementation of the requirements of integrity, availability, confidentiality of information in the process of cross-border transmission should be ensured.

It is assumed to set the range of concepts, the main ones are the concepts of electronic document, as an object of cross-border exchange of documents and recipients, as subjects (subscribers) exchange.

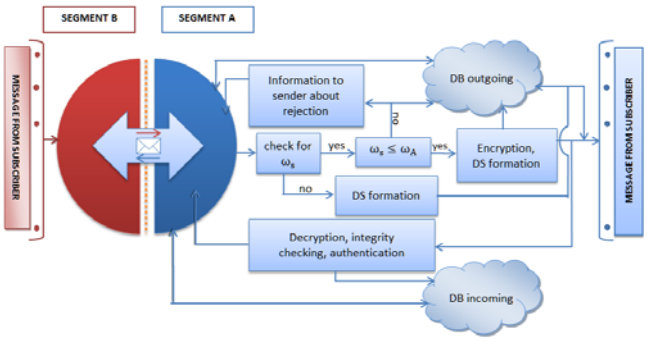

FIGURE I. STRUCTURAL SCHEME OF SEGMENT IN THE INTEGRATED SYSTEM (ω_A – CLEARANCE LEVEL OF SUBSCRIBER, ω_S- SECURITY LABEL OF MESSAGE)

Interacting sides have different cryptographic information protection standards consequently the information exchange between sides "A" and "B" are transmitted in plaintext over the secure channel in the integration gateway.

The message *M* that contains header (information about the sender, address, route, date and time label of sending and receiving, security label and other) in plaintext is sent to integration gateway from the side "B".

The security label in the message header provides information about the confidentiality of message content, and allows to restrict the list of recipients, which can open, forward, send the message. Security label for objects ω_S (degree of confidentiality of information) have the following categories: Top Secret, Particularly Important; Top Secret; Secret; public information.

Clearance levels for subject ω_A have the following categories:

- Level 0 (general use);

- Level 1 (official use);

- Level 2 (limited use);

- Level 3 (secret);

- Level 4 (top secret).

Backup with headers are recorded and stored in the incoming and outgoing databases (DB) respectively. Received message *M* in plaintext is checked for Security Classification and the possibility of transmission to the subscriber of side "A". If there is the security label then the message is encrypted and is signed with digital signature, otherwise the message is only signed by the DS.

The subscriber is entitled to receive only the documents which the security labels do not exceed its own clearance level: $\omega_S \le \omega_A$. If the subscriber clearance level does not exceed security label of message: $\omega_A \le \omega_S$ then encrypted message with the digital signature is not transferred to subscriber. Message sender is sent information about the reason of refusal, i.e., "Information about the rejection to the sender". The message data is sent to the DB of outgoing objects for the solving possible conflict situations.

IV. Modeling of Cryptographic Means of Information Security for the Integrated System

One of the requisites of the electronic document is a digital signature. Implementation of legal function of the electronic document is provided by the requisites of the document. Such signature is used to identify the person who signed the transmitted electronic document and also for establishing the absence of changes in the document after it was signed.

In connection with this allocates the certification authority (department or external organization) which generates for each user so-called "key certificates" with the help of specialized software. DS key consists of a private key and a public key.

In the cross-border exchange of information, each of the interacting sides is developing their national cryptographic means. Cryptographic encryption and digital signatures is developed using the algebraic approach and based on nonpositional polynomial notations systems (NPNs) or polynomial number systems in residue classes (polynomial RNS) are the basis for the creation of the cryptographic means in the proposed model [5].

The digital signature system, developed on the basis of DS systems with the public key and NPNs is used in the proposed model of interaction of the sides. Application of NPNs allows creating effective cryptographic systems of high reliability, which enables the confidentiality, authentication and integrity of stored and transmitted information [6-7]. In the development of unconventional asymmetric cryptographic systems the length of keys is significantly reduced without loss of cryptographic strength.

V. SUMMARY

In developing the model of protected cross-border information exchange is taken into account the technological features of such interaction and the legal issues of ensuring the legal significance of electronic information in integrated system. The results of research are used in the implementation of the national segment model and will contribute to the development of the domestic means of information security ensuring.

ACKNOWLEDGEMENT

Authors express their deep appreciation to the Committee of Science, Ministry of Education and Science of the Republic of Kazakhstan, for the funding of the research.

REFERENCES

[1] Sazonov A.V. Subjects and technology rights management infrastructure in transboundary space // General information security concerns and objects №3, 2012, C.83-87.

[2] The concept of using in interstate information service interactions and legally binding electronic documents // http://www.tks.ru/news/law/2014/10/08/0006.

[3] Problems of public policy of regional development of Russia / Proceedings of the Scientific Conference. - The scientific expert, M., 2008. - p. 1080.

[4] Model Law on cross-border information exchange of electronic documents // http://www.pvti.ru/.

[5] Akushskii, I.Ya. andJuditskii, D.I.: Machine Arithmetic in Residue Classes [in Russian], Sov. Radio, Moscow (1968), 439 p.

[6] Bijashev, R.G. and Nyssanbayeva, S.E.: Algorithm for Creation a Digital Signature with Error Detection and Correction //Cybernetics and Systems Analysis. №4, 2012, PP. 489-497.

[7] Biyashev R., Nyssanbayeva S., Begimbayeva Y., Magzom M. Modification of the Cryptographic Algorithms, Developed on the Basis of Nonpositional Polynomial Notations //Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015), Vienna, Austria, 2015, PP.170-176.