Research Article Open Access

R. G. Biyashev, S. E. Nyssanbayeva, and Ye. Y. Begimbayeva*

Development of the model of protected cross-border information interaction

DOI 10.1515/eng-2016-0025
Received May 04, 2016; accepted Jun 22, 2016

Abstract: This article investigates a proposed model of cross-border exchange and information security in the cross-border interaction in the integration system. A structural scheme of protected cross-border information exchange is proposed. Cross-border interaction of sides for information exchange in the integrated system is provided by the creation and use of the integration segment and national segments. The main tasks of a trusted third party are formulated. The model of sides' interaction scheme of the integration system using the integration gateway is presented. In this paper, a model of modified nonconventional digital signature system based on the scheme of the Digital Signature Algorithm and nonpositional polynomial number systems (NPNs) are described. Application of NPNs allows creating effective cryptographic systems of high reliability, which enables the confidentiality, authentication, integrity of stored and transmitted information.

Keywords: cross-border information exchange; information security; digital signature; nonpositional polynomial number systems

1 Introduction

Today, due to globalization of world integration processes, information interaction specifically cross-border interaction, using information and telecommunication systems are an essential element of the relations of society. In this interaction, a number of organizational and legal questions of ensuring protection and trust appears. One of the important problems in cross-border information interaction or exchange is ensuring information protection using such systems.

Cross-border information interaction or exchange – the information transmission to the operators through the borders of states to the authority, person or legal entity of the state.

On September 18, 2014 the Council of the Eurasian Economic Commission approved the Concept of use in interstate information service interactions and legally valid electronic documents [1]. The Concept documents the need to ensure legal validity of electronic documents in the cross-border information exchange.

Earlier in 2008 the decision of the Council of Commonwealth of Independent States (CIS) Heads of State approved the concept of cooperation - the CIS in the field of ensuring the information security. In the purposes of cooperation at performance of the provisions of the Concept in 2012 the Agreement on cooperation of states - participation of the CIS in the field of ensuring information security was accepted. Agreement indicates the necessity of organizing the cross-border information transmission, convergence of the legal and regulatory acts and regulatory guidance documents of member States, regulating relations in the field of ensuring the information security.

In this regard, questions of strengthening trust and security among the interacting sides in the information process come to the fore. Taking into account the cross-border nature of ensuring issues it requires further improvement of the international cooperation in this area, consistent with the principles of equitable international information exchange.

This is due to the fact that the problem of equal participation of the Republic of Kazakhstan in the international information exchange and in the processes for international regulation of information security is realized.

R. G. Biyashev: Institute of Information and Computational Technologies of MES RK 125 Pushkin str., Almaty, 050010, Republic of Kazakhstan; Email: brg@ipic.kz
S. E. Nyssanbayeva: Institute of Information and Computational Technologies of MES RK 125 Pushkin str., Almaty, 050010, Republic of Kazakhstan; Email: sultasha1@mail.ru
***Corresponding Author: Ye. Y. Begimbayeva:** Institute of Information and Computational Technologies of MES RK 125 Pushkin str., Almaty, 050010, Republic of Kazakhstan; Email: enlik_89@mail.ru

2 The cross-border information exchange in the integrated system

Electronic interaction, especially cross-border interaction, involves collaboration of many disparate information systems. Rights management mechanisms are based on different principles and implemented in different ways in each of these systems [2].

Cross-border interaction is the interaction of subjects of different legal fields. Consequently, the unresolved complex of organizational, technological and legal issues of the legal significance of electronic information in the integrated system is one of the major problem in cross-border information interaction (CBII). The main problems of ensuring information interaction is to develop an effective and reliable rights management mechanism of subjects and provide each side of this interaction its own information security and protection of their informational independence.

One of key directions of work on the creation and implementation of integrated information system of the Eurasian Economic Union (EAEU or EEU) are solving 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 [1].

Electronic data exchange between interacting sides in the integrated system is provided by creation and use of the national segments (hereinafter referred to as segment) and integration gateway (hereinafter referred to as gateway). These segments are a set of secure systems of data transmission, included in each interaction side's node in information exchange (Fig. 1).

Legal validity of electronic documents in CBII in the integrated system is confirmed on the basis of service trusted third party (TTP). TTP infrastructure and certification authority (CA) is located in national segments and organized at the level of each interacting sides. The CA provides signature key certificates for interaction of authorized trusted third parties of national segments of the integrated system.

The main tasks of TTP are:

- implementation of authentication of electronic documents and digital signature (DS) of information interaction subjects in a fixed time;
- implementation of the guarantees of trust in cross-border exchange of electronic documents;
- ensuring the legal use of DS in the incoming and outgoing electronic documents and messages, in accordance with the rules and requirements of the law of interacting side, wherein the trusted third party is [3].

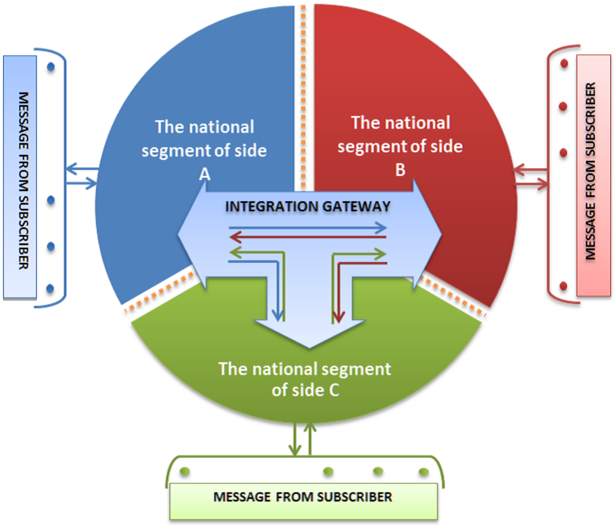
MESSAGE FROM SUBSCRIBER
The national segment of side A
The national segment of side B
INTEGRATION GATEWAY
MESSAGE FROM SUBSCRIBER
The national segment of side C
MESSAGE FROM SUBSCRIBER

Figure 1: The cross-border information exchange in the integrated system

As documents circulate in the cross-border space of trust conflict situations may arise. These situations are connected with formation, delivery, receipt and receipt confirmation of the electronic document, and also with the use of DS in documents. Resolution of conflict situations is included in the tasks of the certification center. Conflict situations arise in the following cases:

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

3 Development of the model of protected cross-border information interaction

The implementation of the structural scheme of the protected CBII use the basic terms and definitions of model law from "On the cross-border information exchange of electronic documents" [3].

The model of interaction scheme between the two sides in the integrated system are proposed. The structural scheme of interaction of the segment of information exchange is shown in fig. 2. 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 be implemented using a special automated system CBII - Integration Gateway.

The 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 means, hardware and software information protection from unauthorized access, and other hardware and software are determined for workstations of each interacting sides. In the information transmission over a secure 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.

In order to develop the methodology of creating an electronic cross-border space of trust 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.

The parts of the national segment of the integrated system are:

- Software and hardware complex of trusted third party (TTP);
- Certification Authority (CA).

Structural schema of interaction of the sides "A" and "B" in the cross-border information exchange is shown in fig. 2. Interacting sides have different cryptographic information protection standards. Therefore, the information exchange between sides "A" and "B" is transmitted in plaintext over the secure channel in the integration gateway.

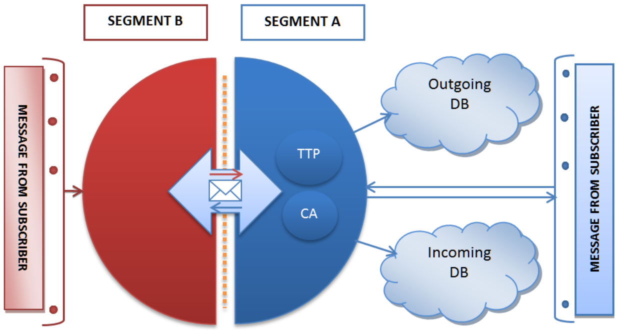

Figure 2: The cross-border information exchange in the integrated system

The message *M* (object) that contains header in plaintext is sent to integration gateway from the side "B". The message header contains information about the sender, address, route, date and time label of sending and receiving, security label and other. Backup with headers are recorded and stored in the incoming and outgoing databases (DB) respectively.

The national segment of side "A" and the exchange of information between the segment and subscriber of side "A" (subject) are considered. Received message *M* in plaintext is sent to the subscriber of side "A".

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 labels for subjects (degree of reliability) and objects (degree of confidentiality of information) have the following categories:

1. Particularly Important;
2. Top Secret;
3. Secret;
4. Confidential;
5. Unclassified.

Certification Authority is checked the presence of the security label. 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 level does not exceed its own level. If the subscriber security label does not exceed security label of message, 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". To solve possible conflict situations, the message data is sent to the database of outgoing objects.

4 Modeling cryptographic means for information protection

The implementation of legal functions of the electronic document is provided by the requisites of the document. One of the requisites of the electronic document is a digital signature. Such a 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.

So-called "key certificates" is generated for each user with the help of specialized software in Certification center (department or external organization). DS key consists of a private key (it is available only to its owner, with its help the owner is signed with a DS) and a public key (it is accessible to all, and determine when and who signed an electronic document).

In the cross-border exchange of information, each of the interacting sides is developing their national cryptographic means. Cryptographic encryption and digital signatures are developed using an 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 [4]. Cryptosystems, developed on the basis of NPNs are called unconventional, nonpositional or modular.

On the proposed model of interaction of the sides the digital signature system, developed on the basis of DS systems with the public key and NPNs will be used.

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 [5, 6]. In the development of unconventional asymmetric cryptographic systems the length of keys is significantly reduced without loss of cryptographic strength.

4.1 Modified asymmetric system of digital signature

Developed unconventional systems of digital signature are basis for creation of the proposed model of the DS [5, 6]. These systems are developed on the algebraic approach base, using nonpositional polynomial notations (NPNs) or polynomial notations in residue classes (polynomial RNS).

In the classical notations in residue number system the bases are prime numbers $p_1, p_2, ..., p_n$, and in RNS a positive integer A is represented by a sequence of residues

$$A = \alpha_1, \alpha_2, \dots, \alpha_n \qquad (1)$$

from dividing this number by the system bases $(p_1, p_2, \dots, p_n)$ [4]. RNS is based on the Chinese remainder theorem [8]. According to the Chinese remainder theorem, representation of A in the form of (1) is unique, in case bases $(p_1, p_2, \dots, p_n)$ are pairwise coprime.

Numbers α_i are formed in the following way:

$$\alpha_i = A - [A/p_i]p_i, i = \overline{1, n}, \qquad (2)$$

where $[A/p_i]$ denotes the integer part of the division A by p_i. From (2) follows, that the number α_i of i-th digit of A is the smallest positive remainder of division A by p_i, and $\alpha_i < p_i$. The range of representable numbers in this case is $P = \prod_{i=1}^{n} p_i$. Here, the range of representable numbers growing as the product of base numbers, and the digit capacity of the number is growing as the sum of the digit capacity of the same base numbers.

Contrary to classical RNS, where the bases are prime numbers, in NPNs (polynomial RNS) bases are used as irreducible polynomials over field $GF(2)$ [7]. Using NPNs allows reducing the length of the key, to improve durability and efficiency of nonpositional cryptographic algorithms [5]. Improving the efficiency is provided by the rules of NPNs in which all arithmetic operations can be performed in parallel to the base module NPNs. In developed nonconventional cryptographic algorithms the formation of digital signature is carried out for an electronic message of the given length. In nonpositional cryptosystems as a criterion of cryptostrength is used cryptostrength of algorithms of formation of digital signature, which is characterized by a complete secret key. Cryptostrength in this case depends not only on the length of a key sequence, but also on choice of a system of polynomial bases. With the growth of the order of irreducible polynomials with binary coefficients, their number also grows rapidly [9]. Therefore, a wide choice of polynomial bases is possible. Cryptostrength of proposed digital signature formation algorithm which using NPNs significantly increases with the length of the hash function [5, 10].

For the process of NPNs formation for signing an electronic message M of length N bits are selected working bases systems with binary coefficients [5, 7, 10]

$$p_1(x), p_2(x), \dots, p_S(x), \qquad (3)$$

where $p_i(x)$ - reducible polynomials over the field $GF(2)$ of degree m_i, $i = \overline{1, S}$ respectively. The main working range in NPNs is a polynomial $P(x) = \prod_{i=1}^{S} p_i(x)$ of the degree $m = \sum_{i=1}^{S} m_i$. The entire selected working base should be different from each other (according to the Chinese remainder theorem), even if they are irreducible polynomials of one degree.

In NPNs any polynomial $F(x)$, which degree is less than m, has nonpositional representation in a form of sequence of residues of its division by the working base numbers $p_1(x), p_2(x), \dots, p_S(x)$ and it is a unique:

$$F(x) = (\alpha_1(x), \alpha_2(x), \dots, \alpha_S(x)), \tag{4}$$

where $F(x) \equiv \alpha_i(x) mod\, p_i(x)$, $i = \overline{1, S}$. The positional representation of $F(x)$ is reconstructed from its form (4) [5, 7]:

$$\begin{aligned} F(x) &= \sum_{i=1}^{S} \alpha_i(x) B_i(x), \\ B_i(x) &= \frac{P_S(x)}{p_i(x)} M_i(x), \; i = \overline{1, S}. \end{aligned} \tag{5}$$

Polynomials $M_i(x)$ are chosen so as to satisfy the congruence in (5).

In NPNs a message of the given length N is interpreted as a sequence of remainders of division of some polynomial (let us denote it as $F(x)$ respectively) by working base numbers $p_1(x), p_2(x), \dots, p_S(x)$ of degree not higher than N, that is, in the form of (4). Base numbers are selected from all irreducible polynomials with degrees varying m_1 to m_S providing that the following equation is satisfied [9]:

$$k_1 m_1 + k_2 m_2 + \dots + k_S m_S = N. \tag{6}$$

At equation (6) $0 \leq k_i \leq n_i, i = \overline{1, S}$, are unknown coefficients and the number of selected irreducible polynomials of degree m_i. One certain set of these coefficients is one of the solutions of (6) and specifies one system of working base numbers, n_i - is the number of all irreducible polynomials of degree m_i, $1 \leq m_i \leq N$, $S = \sum_{i=1}^{S} k_i$ - is a number of selected working base numbers. In the system of working bases the order of these bases is also taken into account. Equation (6) defines the number S of working bases, which produce residues that covers the length N of the given message. Complete residue systems modulo polynomials of degree m_i include all polynomials with the degree not exceeding $m_i - 1$. With growth of degrees of irreducible polynomials, their amount rapidly increases, as a result, the number of solutions of (6) considerably increases.

In the formation of symmetric DS in NPNs the redundant bases are entered: the signed message M is expanded to the redundant bases $p_{S+1}(x), p_{S+2}(x), \dots, p_{S+U}(x)$. These bases are chosen randomly from all irreducible polynomials of degree not exceeding the value of N_k, where $j = \overline{1, U}$. System of redundant bases is formed independently from working bases selecting $p_i(x)$, $i = \overline{1, S}$ but among U redundant bases may coincide with some of the working bases. Denote $a_1, a_2, \dots, a_U$ and $d_1, d_2, \dots, d_U$ degree and the number of irreducible polynomials, respectively, used in their selection. The number of selected redundant bases in this case determined from the equation (the analogue of (5)):

$$t_1 a_1 + t_2 a_2 + \dots + t_U a_U = N_k, \tag{7}$$

where $0 \leq t_j \leq d_j$, $0 \leq a_j \leq N_k$, $j = \overline{1, U}$, t_j - the number of selected redundant bases of degree a_j, $U = \sum_{j=0}^{U} t_j$ – the number of selected redundant bases, which produce residues that covers the hash value of length N_k. Solution of the (7) defines a single system of redundant bases.

Further redundant residues (remainders) $\alpha_{S+1}(x), \alpha_{S+2}(x), \dots, \alpha_{S+U}(x)$ are calculated by dividing reconstructed polynomial $F(x)$ by redundant bases $p_{S+1}(x), p_{S+2}(x), \dots, p_{S+U}(x)$. Then the hash value can be interpreted as a sequence of these residues:

$$h(F(x)) = (\alpha_{S+1}(x), \alpha_{S+2}(x), \dots, \alpha_{S+U}(x)), \tag{8}$$

where $h(F(x)) \equiv \alpha_{S+j}(x) mod\, p_{S+j}(x))$, $j = \overline{1, U}$. The sum of the lengths of redundant residues is the length of hash value and DS.

The ElGamal digital signature scheme [11] is based on the complexity of the problem of computing discrete logarithms in the finite field. DS algorithm is a variation of a digital signature of the ElGamal scheme and K. Schnorr. Reliability of this algorithm is based on the practically insoluble of the particular case of the problem of calculating the discrete logarithm.

DSA is one of the algorithms recommended by the US standard for the DS formation [12]. DSA algorithm is a “classic” example of a DS scheme based on using hash functions and asymmetric encryption algorithms. The strength of the system in general depends on complexity of finding discrete logarithms in the finite field.

The essence of DSA electronic signature scheme is the following. Let sender and recipient of the electronic document in computation of digital signature use large prime integers p and $q : 2^{L-1} < p < 2^{L}$, $512 \leq L \leq 1024$ multiple of 64, $2^{159} < q < 2^{160}$, q - prime divisor of $(p-1)$ and $g = h^{\frac{p-1}{q}} mod\, p$, where h arbitrary integer, $1 < h < p - 1$ such that $h^{\frac{p-1}{q}} (mod\, p) > 1$.

Private key b is randomly selected from the range $1 \leq b \leq q$ and stored in secret. Value $\beta = g^b mod\ p$ is calculated. The algorithm parameters p, q, g are the public key and published for all users of the information exchange system with DS.

Consider the formation of the DS for the message M:

1. hash value h is determined from the signed message $M : h = h(M)$;
2. integer r is chosen by some random method, where $1 \leq r \leq q$, and stored in secret and varies for each signature;
3. value: $\gamma = (g^r mod\ p) mod\ q$ is determined;
4. By using the private key of the sender $\delta = (r^{'}(h + b\gamma)) mod\ q$ is calculated, where $r^{-}1$ satisfies the condition $(r^{-1}r) mod\ q = 1$;
5. Digital signature for the message M is the pair of numbers (γ, δ), which passed along with the message by open communication channels.

DS verification is considered: let denote $M^{'}, \delta^{'}, \gamma^{'}$ obtained by the addressee version of M, δ, γ.

1. the conditions $0 < \delta < q$ and $0 < \gamma < q$ are checking. Reject the signature if any one of the conditions of the digital signature is not satisfied these conditions.
2. hash value $h_1 = h(M^{'})$ from the received message $M^{'}$ is calculated.
3. value $v = (\delta^{'})^{-1} mod\ q$ is calculated.
4. values: $z_1 = (h_1 v) mod\ q$ and $z_2 = (\gamma^{'} v) mod\ q$ is calculated.
5. value: $u = ((g^{z_1} \beta^{z_2}) mod\ p) mod\ q$ is determined.
6. the DS is valid if $\gamma^{'} = u$. It means that in the transfer process the integrity of the message $M^{'} = M$ was not compromised. Otherwise, the signature is invalid.

Modification of the DSA scheme to use NPNs may give increased cryptographic speed.

5 Conclusion

During solving the tasks of ensuring the protected cross-border information exchange, should be taken into account both organizational and technological features of such interaction and the legal issues of ensuring the legal significance of electronic information in integrated system.

Today there is no common model of technology of the cross-border information exchange. The developed model of the technology of protected cross-border information exchange will contribute to the creation of the national segment and development of the domestic means of information security ensuring.

Research in the creation of a modular DS system with the public key is conducted. The modified algorithm of DSA based on NPNs is used in the creating of this system [13]. In the Republic of Kazakhstan the results of research will be used in the implementation of the structural scheme of cross-border information exchange.

Acknowledgement: Research conducted under the grant funding of the Ministry of Education and Science of the Republic of Kazakhstan.

References

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

[2] Sazonov A.V., Subjects and technology rights management infrastructure in transboundary space General information security concerns and objects, 2012, 3, 83–87

[3] Model Law on cross-border information exchange of electronic documents, 2015, http://www.pvti.ru/

[4] Akushskii I.Ya., Juditskii D.I., Machine Arithmetic in Residue Classes, Sov. Radio, Moscow, 1968, 439, (in Russian)

[5] Bijashev R.G., Nyssanbayeva S.E., Algorithm for Creation a Digital Signature with Error Detection and Correction, Cybernetics and Systems Analysis, 2012, 4, 489–497

[6] 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, (15-17 March 2015, Vienna, Austria), 2015, 170–176

[7] Biyashev R.G., Development and research of pass-through method for increase of reliability of data exchange systems in distributed control: Dis. degree for obtaining. Doctor Tech. Sci., Moscow, 1985, 328

[8] Pohst M., Zassenhaus H., Eds., Algorithmic algebraic number theory, New York, NY, USA: Cambridge University Press, 1989

[9] Biyashev R.G., Nyssanbayeva S.E., Kapalova N.A., Private keys for non-positional cryptosystems, Development, research and application. LAP LAMBERT Academic Publishing, Germany, 2014, 126

[10] Nyssanbayeva S.E., Development and research of cryptographic systems based on nonpositional polynomial notations: Dis. degree for obtaining. Doctor Tech.Sci., Almaty, 2009, 240

[11] ElGamal T., A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory, 1985, v. IT-31, 4, 469–472

[12] FIPS PUB 186, Digital Signature Standard, http://csrc.nist.gov/publications/PubsFIPS.html

[13] Biyashev R., Nyssanbayeva S., Begimbayeva Ye., Magzom M. Building modified modular cryptographic systems, Interna-

tional journal of applied mathematics and informatics, 2015, 9, 103–109