Advances in Computer Science Research, volume 89
2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019)

Development and Analysis of Possible Conflict Situations Resolution Systems in an Automated System

Rustem Biyashev[1], Saule Nyssanbayeva[1] and Yenlik Begimbayeva[1,*]
[1]Information Security laboratory, Institute of information and computational technologies of SC MES RK, Almaty, Kazakhstan
[*]Corresponding author

***Abstract*—A model of the protected cross-border information exchange automated system is proposed. The possible conflict situations and the reasons for their occurrence are investigated. An algorithm of actions to resolve possible conflict situations is proposed.**

Keywords—information security; conflict situations; cross-border information exchange

I. Introduction

The widespread digital technologies introduction at the work of public authorities in the interstate digital interaction has led to the need to create and use systems for the cross-border exchange of electronic information. The use of such systems in the interaction between states can significantly reduce the time spent on the documentation exchange, improve and cheapen the procedure of preparing, delivering, recording and storing documents. However, in the case of cross-border exchange of electronic documents, there is an urgent need to ensure the information security of documents, their authenticity, authorship and protection against distortion.

In the cross-border exchange, each automated workstation is the property of one of the interacting parties and is protected by means of protection adopted in the corresponding part. Each party determines for its workplace cryptographic tools, hardware and software tools to protect information from unauthorized access and other hardware and software [1]. Consequently, there is a need to develop the automated system (AS) of protected cross-border information exchange (PCIE).

In the automated system regardless of the presented form of electronic information, various conflict situations may arise. Ensuring non-conflict interaction is an important task for ensuring comprehensive system security. Some of these tasks include research the AS' information objects and security level analysis of the transmitted information in the random and deliberate conflicts. In this regard, there is a need to identify and research possible types of conflict situations and ways to resolve them.

II. Development of the AS PCIE model

The PCIE automated system model involves interconnected subsystems: encryption, electronic digital signature, access control, conflict situations resolution (CSR) systems, and a database.

In the cross-border information exchange of two parties' subjects, the information in open form that comes directly from the integration gateway to the subjects of one side and back is used. One of the variants of the developed model of AS PCIE is presented in Figure 1.

Any received document with a header (information about the sender, recipient, route path, date, departure and receipt time stamp, security label, etc.) with a security label (wm) not exceeding the tolerance level (ws) of the recipient are encrypted and signed with EDS. A document that does not have the security label is signed by EDS. The trusted third party (TTP) verifies the authenticity of the EDS. Document with a negative check or in case of occurrence of conflict situations the system refers to the CSR system.

The access control systems for monitoring information in outgoing and incoming documents for the competent authorities and participants of the cross-border exchange is planned to create. The access control system is designed to provide access to objects classified by various characteristics (degree of importance, degree of secrecy, time, etc.) by subjects that have the necessary authority to do this.

III. Analysis of possible conflict situations in the automated system

Conflict situations are such state of the PCIE automated system in which the possibility of correctly performing at least one of the system tasks (access control, information transfer, encryption, generation and verification of the signature) due to external influence, or internal failures, errors or failure of software or algorithmic support is excluded.

Conventionally, conflict situations can be divided into three categories as a result of:

- Distortion of the input (received) data stream (documents);

- Changes in the system functioning through external intervention (unauthorized access, intentional changes in software or algorithmic support of the system);

- Distortion of the system functions when the input data flow changes (viruses, Trojan horses, errors and software bookmarks).

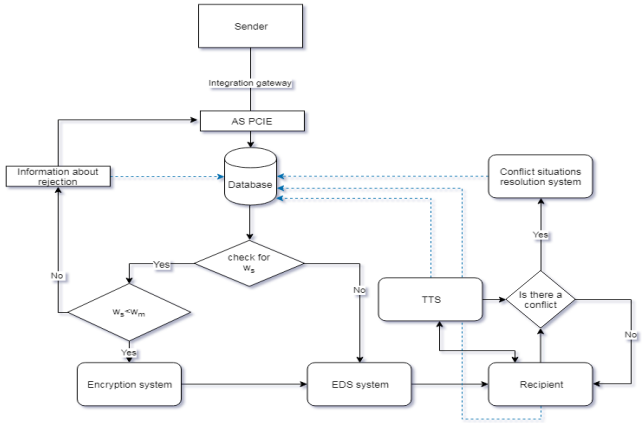

FIGURE I. THE AUTOMATED SYSTEM OF PROTECTED CROSS-BORDER INFORMATION EXCHANGE

Figure 2 shows a structural scheme of the conflict situations resolution system. The CSR system includes the following [2-4]:

– Software agent that collects the necessary data for further analysis. The data source will be the “event log and/or log of sending/receiving documents”, which records all the processes of the automated system;

– CSR mechanism, which processes information from the database and manages the software agent. The result of the module is a decision to make changes to the configuration of the PCIE system to ensure non-conflict interaction based on the rules that are stored in the database.

– Databases that are used to store information about the conflict and the rules of conflict resolution.

Since the AS consists of several connected subsystems, conflict situations may arise in each subsystem. The possible conflicts in the AS PCIE are following.

Dispute between subjects of information exchange in relation to:

1) Fact of sending and / or receipt an electronic document:

- Party's refusal from an electronic document (The Party claims that its sender did not sign an electronic document adopted by the other Party, and the other Party claims the opposite);

- Party’s refusal from facts of receive an electronic document (The party claims that an electronic document sent by it has been received by the other Party, and the other Party claims the opposite).

- Party has no fact of receiving electronic document (The Party claims that the electronic document was sent, but was not accepted by the other Party).

2) The time of sending and / or receipt of an electronic document;

3) The contents of the sent / received electronic document;

4) Electronic document integrity.

Conflict related to:

1) Receipt of a document with EDS with a negative check result;

2) Receipt of a document with EDS with an inappropriate level of tolerance.

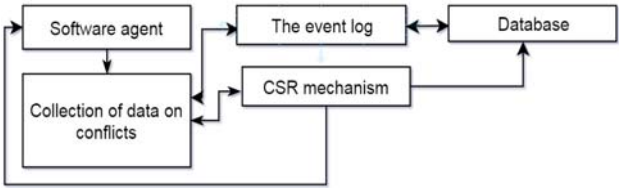

FIGURE II. THE STRUCTURAL SCHEME OF THE CSR SYSTEM

IV. ACTIONS ALGORITHM TO RESOLVE CONFLICT SITUATIONS

The conflict resolution system includes the following steps:

- Verification of the EDS’ archival copy, which is designed to verify the digital signature of the disputed electronic document. If a subject’s public key certificate is not detected in the database, which executed the EDS, the document authorship is impossible. In this regard, the public keys certificates archive must be regularly backed up and stored for the entire set retention period.

- Determination of the formation date of the EDS in the electronic document. The discrepancy between the document formation date and the certificate validity and / or timing of the secret key action does not affect the determination of the document authorship;

- Checking the validity of signature key certificates at the current time;

- Checking for signature key certificate in the list of revoked certificates in the TTP (trusted third party). If the TTP revoked the certificate required to verify the EDS of the document, then the document EDS is considered valid on the document created date and the certificate revocation date.

V. SUMMARY

The proposed conflict resolution system should implement the following functions:

1) Recognize the origin of conflicts, generate corrective action by making changes in the configuration of subsystems;

2) Make recommendations to the user to eliminate conflicts;

3) Maintain an audit of system events to exclude elements that cause conflict. The obtained results will be used to implement the model of the automated system of PCIE.

ACKNOWLEDGMENT

This research was financially supported by the Ministry of Education and Science of the Republic of Kazakhstan.

REFERENCES

[1] R. G. Biyashev, S. E. Nyssanbayeva, and Ye. Y. Begimbayeva The Development of a Structural Scheme of National Segment in a Protected Cross-Border Space // Proceedings of the International Conference on

Wireless Communications, Network Security and Signal Processing International Conference on Advanced Material Science and Environmental Engineering. – 2016. – P. 250-252.

[2] Begimbayeva E.E. The structural scheme and mechanism for resolving conflicts in cross-border information exchange // III International. sci. conf. "Informatics and applied mathematics", dedicated 80th anniversary of prof. Biyashev R.G. and the 70th anniversary of prof. Aidarkhanov M.B. - Almaty, 2018. - P.176-178 (in Russian).

[3] Ding, Y., Guo, X., Su, H., Wang, Z., Zhao, S. Method and system for avoidance of software conflict. US Patent 20070180441 A1, December 22, 2006.

[4] M. A. Polyanichko Polyanichko M.A. Architecture of the system of detection and resolution of the software security conflicts. Izvestiya PGUPS [Proc. of Petersburg Transport Univ.]. 2013, no. 1(34), pp. 39–45 (in Russian).