Implementation of digital signature technology to improve the interaction in company

Anastasia Khrykova[1], *Marina* Bolsunovskaya[1], *Svetlana* Shirokova[1,*] and *Andrey* Novopashenny[1]

[1]Peter the Great St. Petersburg Polytechnic University, Polytechnicheskaya, 29, 195251, Saint-Petersburg, Russian Federation

Abstract. This article discusses the business process of reconciling a memo and improving it using digital signature technology. The technology of business process modeling is applied. Business process models are constructed for their analysis and improvement. The AS-IS and TO-BE process was modeled, the general requirements for the digital signature module were identified, and the possibility of introducing this module into the existing electronic document management system was considered. The features of the project for the oil and gas industry are considered. The necessity of implementing the technology is justified and the effectiveness of its application is shown. The project of introduction of digital signature technology is considered. The goals, tasks, and stages of the project are defined. The advantages of using this technology are described. An important conclusion is made that a digital signature allows you to free up resources for solving key tasks of the company.

1 Introduction

The levels of achievement of the organizational goals of any company reflect the effectiveness of the enterprise management information system, especially with regard to human resources management aspects. Increasing the productivity of each employee reduces the cost of services and improves the quality of their provision. Rapidly developing information technologies help solve these basic problems.

The key to stable operation and continuous development of companies and enterprises is a streamlined process of paperwork. Electronic document management systems are able to adapt to the needs of users or the scope of the company, which significantly increases productivity and work efficiency.

For successful operation of the systems, their constant improvement and improvement is required, which would make it possible to fully satisfy the changing and increasing user requirements [1].

In this regard, it is advisable to pay attention to improving the process of working with documents through the development and implementation of a new module for digital signature of electronic document management system.

* Corresponding author: swchirokov@mail.ru

A digital signature in electronic documents is put in the same case as in paper. An electronic signature is used to confirm the identity of the signatory of information, including documents, emails, source code, etc.

2 Materials and methods

The object of study of this work is company N - an enterprise in the oil and gas industry and its activities in terms of electronic document management [2].

The subject of the work is the electronic document management system used at the enterprise.

The purpose of this study is to refine the electronic document management system to the requirements of users (employees of company N), which consists in developing a new module and its implementation (fig. 1).

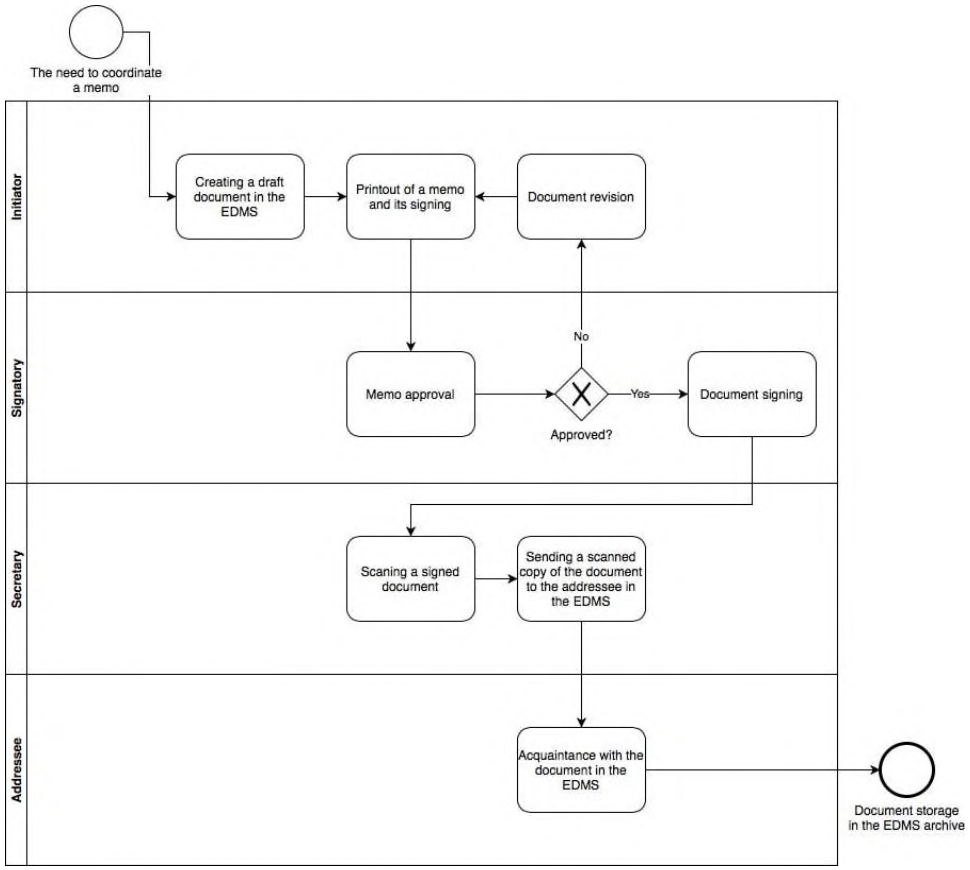

Fig. 1. AS-IS model of a business process.

Company N, an oil and gas company, has long used the American “Documentum” system as an electronic document management system. In connection with the imposition of sanctions against the Russian Federation in 2014, the management of the company decided to switch to the domestic electronic document management system in order to reduce the risks associated with the use of imported software. The basis was taken on a proprietary system that was successfully implemented in the basic configuration.

One of the requirements for the new electronic document management system was the possibility of using an electronic signature to sign company documents. It was decided to add this functionality later, after transferring all documents and processes to the new system [3].

At the moment, the process of signing a memo at the enterprise can take up to 5-7 days. The abundance of scanning and printing operations complicates the process of storing documents, in different departments duplicate documents are often formed.

To solve this problem, it is proposed to finalize the system, develop and introduce an electronic signature module, which will reduce the amount of paper work, documents signed with such a signature will be stored in an electronic archive after approval (fig. 2).

Also, such a module can reduce the time resources spent on this process. Instead of a few days, signing a document will take only a few hours.

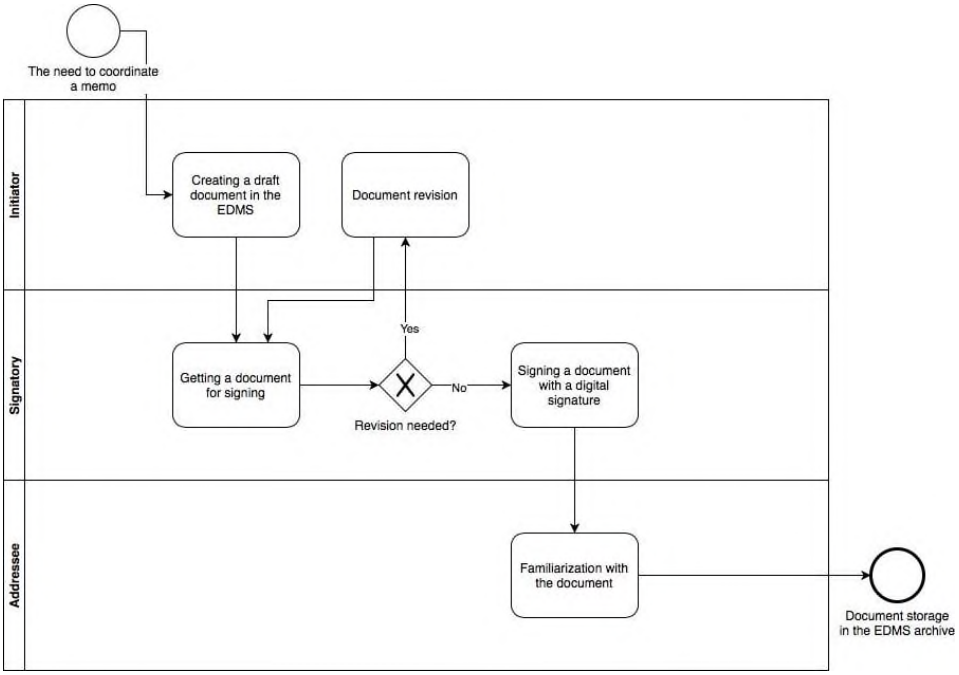

Fig. 2. TO-BE model of a business process.

3 Results

The aim of the project is to develop an electronic signature module to enable electronic signing of internal documents in the electronic document management system, which is unique to handwritten signing of a paper version of a document.

To determine the general requirements for the project, it is necessary to consider the concept of electronic signature, equivalent to the handwritten signature of a document, from the point of view of legislation.

Electronic signing of information stored in electronic form is recognized as equivalent to handwritten signing of a document on paper if [2]:

1. The document is signed with a simple or enhanced electronic signature.

2. There are normative acts or agreements that do not contradict the law, in which there are cases when a document signed with an electronic signature is recognized as equivalent to a document on paper signed with a handwritten signature.

3. The federal legislation and / or regulatory acts do not establish a requirement to draw up a document exclusively on paper.

The first item directly affects the requirements for the information system. Let's consider it in more detail.

Two types of electronic signatures are allowed: simple and enhanced [3]. A simple electronic signature is an electronic signature that, through the use of codes, passwords or other means, confirms the fact that an electronic signature is generated by a certain person. Applicable to projects, this means that the electronic document management system uniquely identifies the user, for example, by his individual login and password, and as a result of the actions for electronic signing of the document, creates a record in the system containing the unique identification data of the document and the user who signed the document.

A simple electronic signature has significant disadvantages:

1. Any user with access to the system database can create a document signing record. However, he does not need to know the password of the signatory.

2. Any user who has administrator access rights in the system can change the signed document and hide information about the fact of the change.

Since in this case any document in the electronic document management system can theoretically be compromised, this complicates the use of information from the system to resolve contentious issues and as evidence in court.

To solve this problem, an enhanced electronic signature is used. Signing in this case is encryption of information with a private key, which only the owner of the electronic signature possesses. Most often, the calculated hash sum of the file or line is encrypted. The resulting encryption result is an electronic signature. As a result of its use:

1. You can uniquely identify the user by his private key. Currently, for this purpose, personalized electronic certificates are used, the issuance and verification of which is carried out by certification centers. Such certificates also allow you to determine the validity and scope of the electronic signature.

2. You can be sure that the document has not been modified by decrypting the electronic signature and comparing the received hash with the hash of the document signed by this signature.

3. An electronic signature is a separate, unique system object that can be uploaded as a file and transmitted via communication channels. At the same time, another information system, in the presence of an electronic signature file and a file with a signed document, can verify the authenticity of the electronic signature and document using its own means.

The use of such a signature, in the presence of regulatory documents regulating its use, makes it possible to conveniently store, transmit and use information from the electronic document management system for resolving disputes and as evidence in court.

Thus, the use of an enhanced electronic signature in the electronic document management system for signing electronic documents seems to be most appropriate.

It is worth noting that an enhanced electronic signature is divided into qualified and unskilled [3]. Their main difference from each other is that the issuance and use of a qualified electronic signature is controlled by the state, and such signatures are used to work with state information systems. In the case of the project under consideration, it is sufficient to use an unqualified electronic signature.

Summing up, the general characteristics of the project can be formulated as follows [4]:

1. In the electronic document management system, there should be the possibility of signing electronic documents with an enhanced electronic signature.

2. There should be the possibility of unambiguous identification of a user using an electronic signature.

3. At company N, it is necessary to ensure the implementation of regulatory documents and legislation in which information signed with an enhanced electronic signature in the electronic document management system will be recognized as equivalent to a paper document.

4. It is necessary to minimize the possibility of compromising the user's private key.

It is proposed to implement the described solution for the business process “Coordination of a service note”, for other business processes the functionality is similar. The proposed solution is designed with the expectation of the possibility of further increasing functionality with minimal modifications [5].

For full use of the electronic signature, Company N must have a root certification authority and an intermediate certification authority based on the Active Directory certification services that are part of the Windows Server operating system; Windows Server-based domain controller using Active Directory implemented electronic signature tools (fig.3).

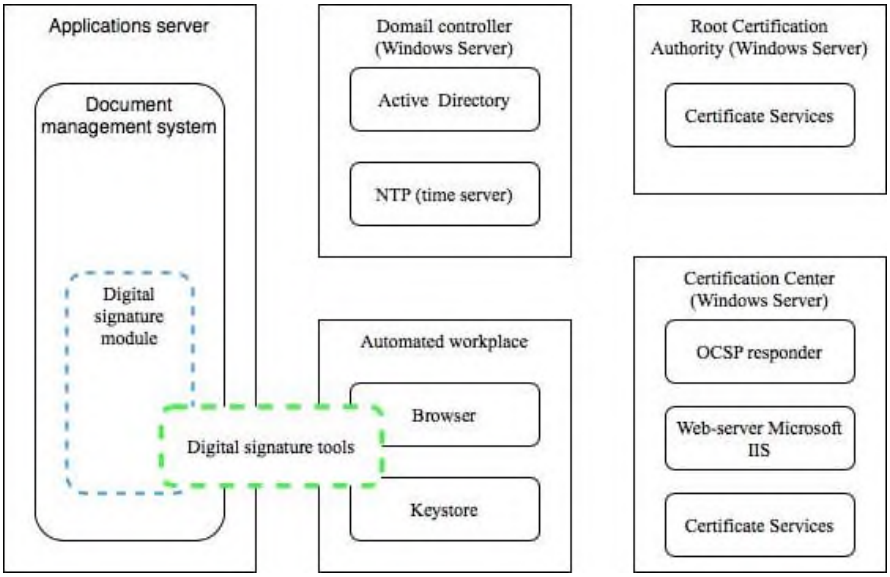

Fig. 3. Project's product structure.

The root certification authority is used to sign the certificate of the intermediate certification authority and its own. These certificates are distributed by Active Directory to all computers in the domain as trusted.

An intermediate certification center carries out [4-6]:

- Issuance of certificates and key pair for users;
- Revocation of certificates;
- Publication of a list of revoked certificates;
- Acts as a defendant OCSP (Offensive Security Certified Professional) - responds to requests for certificate verification, returning its current state (valid, revoked, not found) [7];

Using an intermediate certification authority, templates for issued certificates are generated and published in Active Directory.

The domain controller manages Active Directory services, is responsible for authorizing users by domain login and password, and acts as a time server [8]. When forming an electronic signature, the electronic document management system requests the current date and time, which are added to the signature.

Means of electronic signature include:
- Electronic signature module;
- Add-on for the CryptoPro Browser Plug-In browser;
- Cryptographic provider.

CryptoPro Browser Plug-In is a ready-made free product [9]. It is proposed to use Microsoft Enhanced Cryptographic Provider v1.0, which is part of the Windows operating system, as a cryptographic provider.

On the side of the electronic signature module, data is prepared and a hash is generated, and it is also possible to verify the electronic signature on the server. The browser add-on implements data transfer between the cryptographic provider and the electronic signature module, forming the latter. The cryptographic provider performs the encryption operation with the private key [10].

All work with the private key and cryptographic operations are carried out at the user's workstation, the transfer of the hash amount and electronic signature between the client and the server is encrypted using the HTTPS protocol.

4 Discussion

Thus, after carrying out this work, the business process of approving the memo was analyzed, and the possibility of finalizing the electronic document management system using the digital signature module to increase the efficiency of interaction between company employees was revealed. Various options for electronic signatures were considered and the most suitable one was selected, which satisfies both the requirements of the customer and the legislative aspects [11]. Electronic signature is a simple, but at the same time powerful tool that can reduce the time spent on processing internal documentation and free up labor resources for more important tasks of the enterprise.

5 Conclusions

In the modern world, no enterprise that plans to launch a new product or service on the market that not only wants to remain on the market, but also occupies a leading position that wants to automate the functioning process, cannot exist without any software. And we are talking about information systems [12]. The purpose of information systems can be different, it all depends on what goal the management of a company pursues.

Sooner or later, the organization begins to think about the automation of workflow and the transition to its paperless version, as well as the introduction of electronic signatures. Some introduce electronic signatures as a tribute to fashion, others because the law so requires, and still others because they have analyzed business processes, weighed risks and costs, and determined why this is necessary [13,14].

A digital signature allows you to reduce the labor costs of processing documents, reduce the costs of working with documents and free up resources for the key tasks of the company.

References

1. V.N. Volkova, V.N. Kozlov, V.E. Mager, L.V. Chernenkaya, *Classification of methods and models in system analysis*. *Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM 2017, p. 183–186, 7970533*, (2017)

2. V. Volkova, G. Gorelova, N. Pankratova, *The Development of the Cyberphysical System Concept on Base of the Interdisciplinary Theories. 2020 IEEE 2nd International Conference on System Analysis and Intelligent Computing, SAIC 2020, 9239213* (2020)
3. A.P. Antonov, A.S. Filippov, O.V. Mamoutova, *Next generation FPGA-based platform for network security Conference of Open Innovation Association, FRUCT, 2016-September, p. 9–14, 7561501* (2016)
4. M. Bolsunovskaya, S. Shirokova, A. Loginova, M. Uspenskij, *The development and application of non-standard approach to the management of a pilot project. In: IOP Conference Series: Materials Science and Engineering* (2019) https://doi.org/10.1088/1757-899X/497/1/012024
5. A.A. Daukaev, M.S. Magomadov, *About the origin of the term "oil", early mentions and practice of oil production. Modern problems of Geology, Geophysics and Geoecology of the North Caucasus, 118-122* (2011) URL: https://elibrary.ru/item.asp?id=21225076
6. R.E. Kalman, *A new approach to linear filtering and prediction problems,* Journal of Basic Engineering **82**, 35-40 (1960)
7. *Gazprom Neft conducts automation and unification of the business process based on the materials of Gazprom Neft,* Oil and gas vertical **11**, 114-116 (2008) URL: https://elibrary.ru/item.asp?id=11584344
8. M.B. Uspenskij, S.V. Shirokova, O.V. Mamoutova, V.A. Zhvarikov, *Complex Expert Assessment as a Part of Fault Management Strategy for Data Storage Systems,* Lecture Notes in Networks and Systems **95**, 592-600 (2020) https://doi.org/10.1007/978-3-030-34983-7_58
9. M.Yu. Ermolenko, *Integrated business planning as minimization of uncertainty through multi-level planning, Establishment of the Russian Academy of Sciences V. A. Trapeznikov Institute of management problems of the Russian Academy of Sciences. Under the General editorship of S. N. Vasiliev, A. D. Tsvirkun, 266-267* (2009) URL: https://elibrary.ru/item.asp?id=26325728
10. A.K. Kurmanbek, S.S. Noorzad, *Developed a system of criteria of information security when implementing information systems,* New science: from idea to result **5-2** (84), 175-178 (2016) URL: https://elibrary.ru/item.asp?id=26104550
11. M. Bolsunovskaya, S. Shirokova, A. Loginova, *State of current data storage market and development of tools for increasing data storage systems reliability*, E3S Web of Conferences **135**, 04076 (2019)
12. G.I. Solomatin, O.V. Belousov, A.A. Korotenko, *Integrated information system of oil and gas production OIS+,* Oil industry **10**, 36-39 (2003) URL: https://elibrary.ru/item.asp?id=17746170
13. I.P. Simakov, P.V. Kholodnykh, *The development of theoretical and methodological foundations, mathematical methods and software to analyze the reliability, security and survivability of structurally complex technical systems, In: Proceedings of the 9th conference on management "Information technologies in management (ITM-2016)", p. 244-254*, St. Petersburg (2016)
14. T. Yang, H. Jiang, D. Feng, Zh. Niu, K. Zhou, Y. Wan, *DEBAR: A scalable high-performance de-duplication storage system for backup and archiving. In: Proc. IEEE International Symposium on Parallel & Distributed Processing (IPDPS), pp. 1–12. IEEE* (2010). DOI:10.1109/IPDPS.2010.5470468