PROTECTION OF ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS AND FINANCIAL SYSTEMS

Sharipova U.B.
Samarkand branch of Tashkent University of Information Technologies named after Mukhammad al-Khwarizmi umka_azi@mail.ru

P. F. Nasriddinova
Samarkand branch of Tashkent University of Information Technologies named after Mukhammad al-Khwarizmi umka_azi@mail.ru

The work of modern companies is unthinkable without an effective system of electronic document management (EDMS), allowing to optimize the formation, processing, transmission and storage of corporate documents. An EDMS may also be tasked with ensuring the legal significance of electronic documents. The legal value of an electronic document is ensured by an electronic signature. The order of use of EDS in corporate information systems can be established by the enterprise or the agreement between the participants of electronic interaction.

Enhanced EDS must be obtained as a result of cryptographic transformation of information using the electronic signature key, ensures the integrity of an electronic document and allows to identify the person who signed it. Enhanced qualified electronic signature (qualified signature) additionally implies the use of qualified certificates, as well as means of generation and verification of the signature meeting special requirements.

From a cryptographic point of view, it is assumed the use of asymmetric cryptosystems based on PKI public key infrastructure.

The use of an enhanced qualified signature equates a signed electronic document to a handwritten hard copy document. Electronic documents authenticated with other types of signatures may be legally valid by agreement of the parties. Only reinforced qualified EDS is used in state information systems.

Another task of EDMS may be to ensure confidential document flow, which includes, among other things, the encryption of electronic documents in their storage and transmission. Document encryption is usually provided by symmetric cryptosystems.

Enhanced EDS must be obtained as a result of cryptographic transformation of information using the electronic signature key, ensures the integrity of an electronic document and allows to identify the person who signed it. Reinforced qualified electronic signature (qualified signature) additionally assumes the use of qualified certificates, as well as means of generation and verification of the signature meeting the special requirements from a cryptographic point of view is supposed to use asymmetric

cryptosystems, based on the PKI public key infrastructure.

The use of an enhanced qualified signature equates a signed electronic document to a handwritten hard copy document. Electronic documents certified by other types of signatures may be legally valid by agreement of the parties (the parties to electronic interaction must have adopted the relevant regulations and/or agreements in advance). Only reinforced qualified EDS is used in state information systems.

Another task of EDMS may be to ensure confidential document flow, which includes, among other things, the encryption of electronic documents in their storage and transmission. Document encryption is usually provided by symmetric cryptosystems.

Thus, under the system of secure document management (secure EDMS) is usually understood as a system of legally relevant electronic document management, ensuring confidentiality, integrity and protection of the processed electronic documents. In this case, their protection is understood as the inability to send a false electronic document on behalf of a legitimate user of the system.

Secure legally significant electronic document flow is used for:

- organization of collective work with documents in geographically distributed corporate information systems;

ensure confidentiality and integrity of documents; confirm authorship (authenticity) of documents and impossibility to deny authorship; ensure users' confidence in the content of electronic documents SKZI, which includes functions to create and verify electronic signatures, must:

when creating an electronic signature:

- show the person signing the electronic document the content of the information he or she signs;
- create EDS only after the operation to create a signature is confirmed by the person, unambiguously show that the EDS was created;

When verifying an electronic signature:

- show the content of the signed electronic document;
- show information about changes made to the signed electronic document;
- indicate the person whose key was used to sign electronic documents.

In modern conditions, electronic document flow generally goes beyond the corporate limits (for example, companies submit electronic accounting statements to the tax authorities), so the use of a qualified electronic signature is preferable.

Thus, it is impossible to avoid the need to transfer electronic documents over open networks (via the Internet), which may also be due to the geographically distributed structure of the company itself. All this requires the organization of secure VPN-connections, which can be implemented by means of standard secure network protocols (SSL and TLS for transmission on the Internet and IPSec - within the local

network), including, if necessary, based on certified cryptoproviders (CSP) that support cryptographic standards.

A possible structure of a secure EDMS is shown in Fig. 1. Work in the internal network is organized according to the "thin client" principle.

The information protection system includes subsystems:

- user authentication; access control; event logging and accounting; integrity control; user management;
- cryptographic protection.

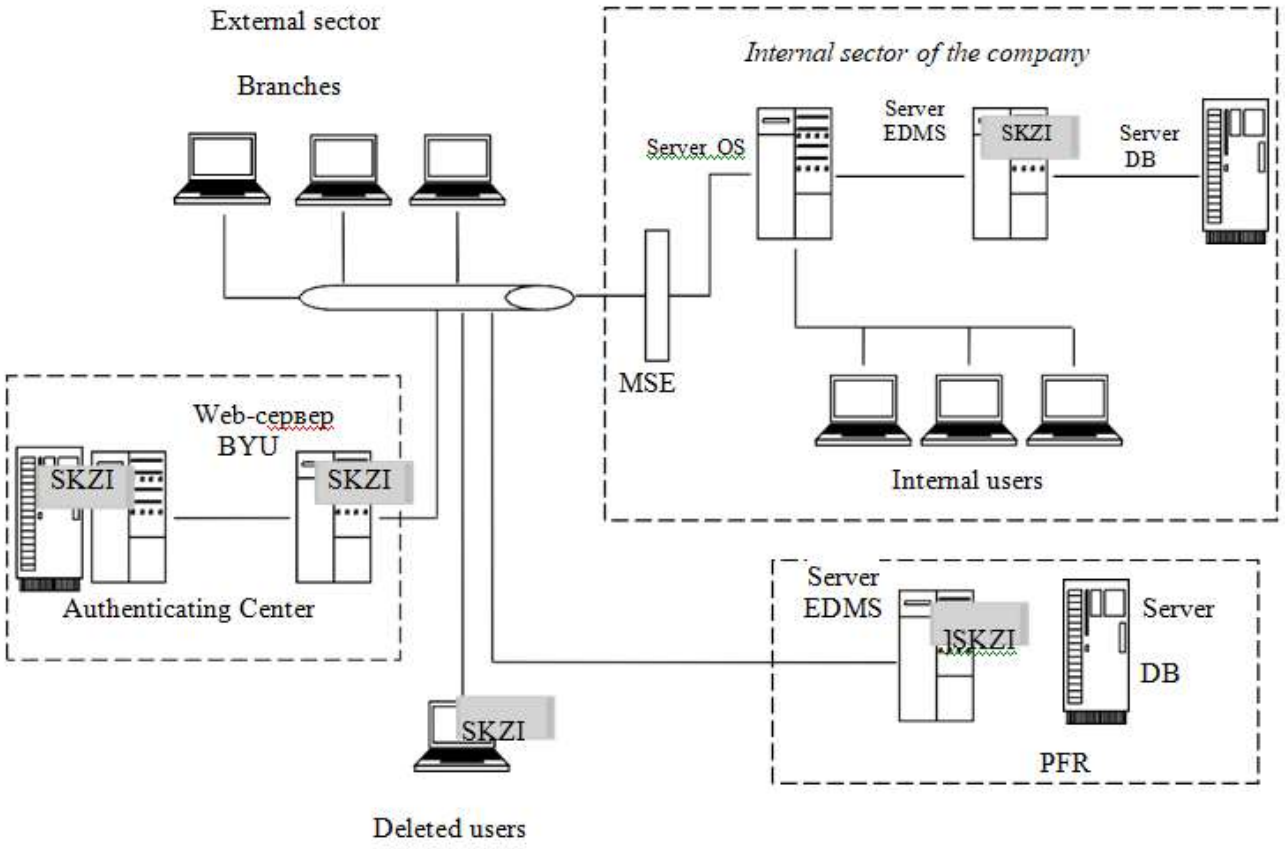

Fig. 1. An example of a secure EDMS

The cryptographic module of the EDMS protection system provides operation with an electronic signature and appeal to a trusted certification center, as well as transparent encryption of information for its secure storage and transmission. It can also be part of the user authentication subsystem, supporting the use of divisible key media (smart cards, USB tokens). This option is preferable because it allows you to store secret keys, used both for authentication and signing documents, on external carriers.

Information systems used in the banking and credit and financial sector and are

characterized by a large degree of modularity and a complex, geographically distributed structure. The SKZI used for the protection of personal data must have a class of at least KS2. The need to use SKZI is determined by the organization.

Electronic payment systems with the use of payment cards must use security features that meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS v.3.0, Payment Card Industry Data Security Standard). PCI DSS provides for the use of strong cryptographic algorithms to protect cardholder data during storage and transmission, as well as the implementation of key management procedures.

It is forbidden to store after authorization: critical authentication data (except card issuers), the full content of the card magnetic stripe, CVC- and PIN-codes, even in encrypted form. PAN payment card numbers are stored using unidirectional hash functions or strong encryption. Secure cryptographic algorithms and security protocols (e.g., SSL/TLS, IPSec, SSH, etc.) are used to transfer data over public networks using only trusted keys and certificates. Strong encryption must also be provided when using wireless networks.

References

1. Recommendation X.800. Data networks: open systems interconnection (OSI); security, structure, and applications.. A risk-free architecture for the interconnection of open systems for ICCTT applications. - Geneva, 1991 [Electronic resource].
2. Burnett S., Payne S. Cryptography. The official guide to RSA Security. - Moscow: OOO "Binom-Press", 2009.
3. M. Mamaev, S. Petrenko Technologies of information protection in the Internet: A special reference book. - SPb: Peter, 2001. – p.848.
4. Schneier B. Applied Cryptography: Protocols, Algorithms, C source code. - Moscow: Triumph, 2012. – p.816.