Makrufa Sh. Hajirahimova
Institute of Information Technology, ANAS, Baku, Azerbaijan
makrufa@iit.ab.az
DOI: 10.25045/jpis.v06.i2.06

SOME ASPECTS OF THE SECURITY OF ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS

One of the broadest application fields of information-communication technologies (ICT) is clerical work. Beginning in the 1990s, the application of computer systems in electronic document management allowed clerical work to be performed electronically with the application of information technologies (IT). This article describes the security issues of these systems, which have become an important factor in the solution of management issues. The main factors necessitating the security of electronic document flow systems are identified, the classification of threats is reviewed, and the main security issues are explored. Last, the technologies for security maintenance in those systems are analyzed.

Keywords: *electronic document, electronic document management system, identification, authentication, electronic digital signature.*

Introduction

The transition to a new format of information, the electronic document (e-document) has resulted from the development of information technologies (IT) and its broad application to all activity spheres. To manage e-documents, computer systems for electronic document management or electronic document flow have begun to be used in both the private and government sectors [1].

The electronic document management system (EDMS) is a technical organizational system for the creation, storage, search and distribution of e-documents, in addition to the management of accessibility and the control over the document flow within an organization [2]. EDMS is a computerized system to organize and manage documents received and sent by an organization and intra-organizational documents, and it is one of the most rapidly developed fields of IT. Regardless of an organization's size, the application of electronic document flow has become a necessity. Although the application of EDMS allows for greater flexibility in processing and storing information and in generating profits, a small mistake may lead to new security threats.

As with paper documents, different privacy levels pertain to e-documents: they are divided into public information and commercial or state secrets. During the application of EDFS in the government sector, the system security measures are important. In general, the application of electronic-digital signatures (EDS) is a necessity for EDMS security [3, 4] because the use of EDS is a guarantee for document security and protection. However, the correct application, infrastructure and expansion of security services for EDS remain a problem. The definition of a secure EDMS is difficult with changing legal frameworks, loopholes in standards, and rapidly developing technology. This requires both the producers and users to pay attention to the improvement of system security. Thus, it is very important to recognize some aspects of EDMS security.

The factors necessitating the security of electronic document management systems

As mentioned in the *DSS Consulting* agency information, the government sector is currently a major consumer of EDMS [5]. Amid the creation and development of the information society and e-government structure, the government has increased the attention paid to EDMS. As in other countries, the development of the electronic state (e-state) in Azerbaijan has led to a new internal organizational mentality based on electronic administration regulation to maintain transparent state services for the general population and business sector. In this regard, the main factors in e-document flow security in Azerbaijan are:

- EDMS has become the most prominent component of e-state infrastructure that is being created and developed. Previously, information systems were developed for use within the organization in government bodies, and currently these systems support electronic communication between government agencies and citizens (G2C), between government and business (G2B)and between government departments (G2G) [2].
- In relation to the establishment and development of e-government structure, the issue of protecting exchanged documents, classified information and private data is important because of the expansion of electronic services in government [6-8];
- As a rule, documents are being processed while being exchanged between different institutions, which must not be accessible to everyone [4];
- In government organizations working with citizens and juridical persons, the completeness and transparency of EDMS information and the importance of applying security tools for maintaining e-document copyrights must be understood [2, 7];
- Adopted regulation on electronic signatures allows for e-document protection and the application of different security technologies in EDMS. As in other countries, regulatory acts adopted in Azerbaijan [4,9] enabled intra-organizational and inter-organizational document flow via EDMS by providing the legal framework for transitioning from paper documents to electronic documents;
- There is a need for e-documents to be regarded as equal to paper documents, and for the maintenance and understanding of legal mechanisms in enterprises and organizations [2].

Previously, the goal was only the security maintenance of documents or information resources; whereas, securely maintaining the system of distribution, processing and storing e-documents has now become the main goal [10, 11]. An EDMS includes several technically complex functional subsystems, certification centers, management centers and so on. An EDMS is created with the help of technical tools with platforms that differ in terms of their architecture and organizational principles for document flow. The issue of the security maintenance of EDMS is impeded by the absence of interoperability (discrepancies) in a technical sense. Hence, a complex approach to the maintenance of system security at all levels is necessary. First, the hardware security (computers, servers, network devices, cables, etc.) must be provided. Thereafter, system files (software, databases, system files, etc.) must be protected. Otherwise, malicious parties may be able to seize EDMS files through file copying or the corruption of the operating system and devices. Last, the security of documents placed in a system must be maintained. While applying this approach, it is possible to be protected from threats at all levels and to establish a secure EDMS. This type of security may be much more expensive compared to the price of EDMS itself. Hence, the balance between security and costs must be considered.

As mentioned before, the documents circulating within the organization can be public or closed. This presents unavoidable threats during the requests of users with or without permission to access the system or document processing tools. Hence, during accessibility management, the access rights of each user must be minimized and considered based on the principle of the official functions they perform. At this stage, the application of EDS as a mutual authentication mechanism is necessary. In this regard, a public-key infrastructure must be established, and a secret-key system with strong security tools must be used.

The classification of threats to electronic document flow systems

Different threats may occur during electronic document management. Usually, the main threats to EDMS are classified as follows:

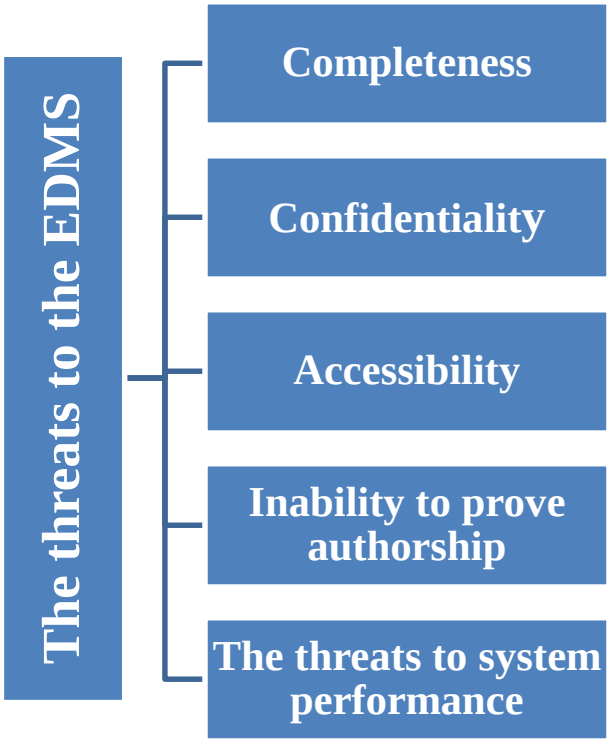

Figure 1.Threats to EDMS

- A completeness threat is to damage, destroy or distort the information accidentally or deliberately.
- A privacy threat is any kind of privacy violation such as information theft, seizure, and change in route.
- Accessibility. This threat is the violation of access to required information for users within a reasonable period of time.
- The impossibility of authorship evidence is expressed as a hardship in proving that a given document was created by a particular user when EDS was not used. This disables the document flow from a legal standpoint.
- The threats to system performance or efficiency include a deliberate attack, or disruption in system performance due to a user's actions or when equipment and software maintenance is disrupted.

Thus, security measures against threats must be applied throughout the entire EDMS, including mechanisms to prevent a third party from reviewing e-documents without permission in the system, the unambiguous authentication of an e-document sender, the protection against e-document modification without permission and conflict solution. The first three are solved with the help of cryptographic and coding algorithms (RSA, EGSA, DSA, ECDSA, etc.) [3,12,13]. The last one is solved in accordance with the regulations for e-document exchange among system participants [4].

Security aspects of electronic document management systems

With the development of IT, the threats against e-documents are increasing such that technical and organizational opportunities have increased for forgery, the illegal seizure of e-documents or routing changes by malicious parties, and access to e-documents without

permission. Several cases of backdating or altering documents have occurred [2,12]. The main issue is that a secure EDMS is necessary for the conventional protection of an information system [10]. As such, important issues for document protection among EDFS users include the application of mechanisms such as users' authentication, access rights, the approval of e-document authorship, control over e-document completeness, privacy and control over software maintenance for legal framework compliance, cryptographic algorithms and antivirus programs.

Users' authentication is the verification of identity with the help of cryptographic conversion. Authenticity reflects two features: completeness—a document must be protected without altering it—and the identification of the document's sender or authorship verification. Authentication technologies that have been applied include authentication tools (biometric data such as handprints, eye scanning, and voice recognition). Although attractive because the user does not need to have a smartcard or to memorize a PIN code, this technology is expensive and does not provide the required reliability level. The most reliable identification is authentication. Authentication allows the sharing and personalization of access by requiring all users to maintain personal credentials and be responsible for activities performed while using those credentials. To personalize access, the public key infrastructure (PKI) [14] is a mechanism for checking the authentication and completeness of a signed document. In short, the main issues for a secure EDMS are a strict authentication of users for security, access to important information resources, restricted access to private information and personal data, blocking interventions that occur without permission and the provision of access to general public information.

Infrastructure issues. Infrastructure elements in maintaining a secure electronic document flow are the following [12,15-22]:

- The electronic base infrastructure of documents;
- EDS infrastructure, including a competent certification center with a unified system based on public key infrastructure;
- Run-time infrastructure for time stamping documents, trust-service infrastructure for determining trusted third parties and the point of document publishing (Figure 2);
- Electronic registry infrastructure for the legal status of participants of mutual information exchange and the verification of competences and signature rights.

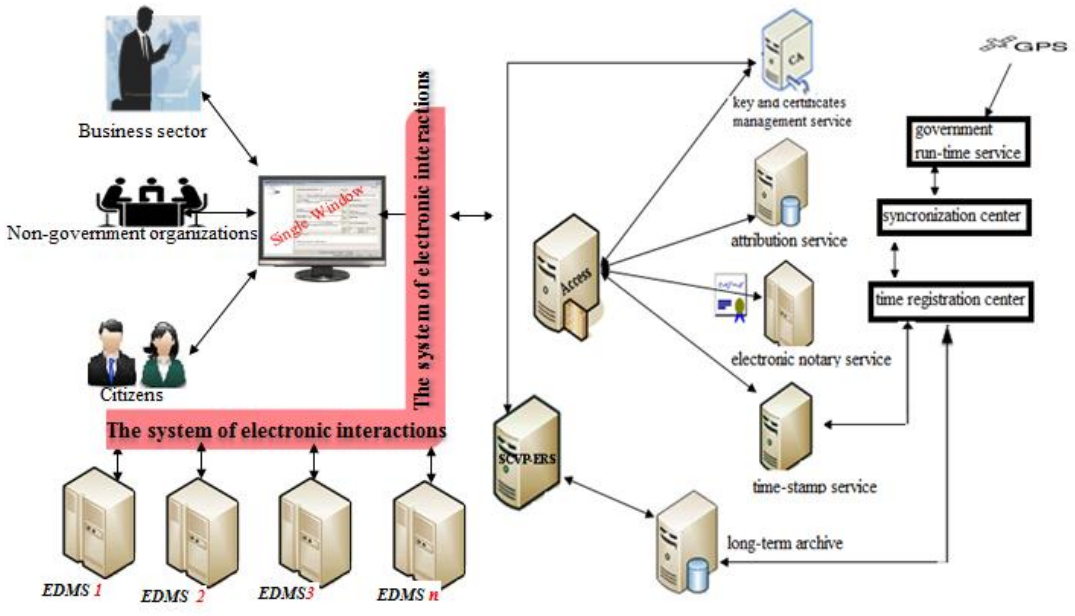

Figure 2.Trust services infrastructure to documents

Trust-service infrastructure must be established based on international standards and recommendations. The technical concept of this infrastructure is expressed in the ITU-T recommendation from the X.842 series of the International Telecommunication Union [15]. In X.842, the recommendations for trust services are specified, directions on infrastructure management are presented and the roles and responsibilities of persons using trust infrastructure and those services are determined. The format of the public key certificate used here is in accordance with the ITU X.509 [16] recommendation. The format of the improved digital signature (IDS) used is based on the standard of the European Telecommunications Standards Institute (ETSI), RFC 5126"CMS Advanced Electronic Signatures (CAdES)" [17]. The application of IDS allows for unambiguous specification of the signature date of e-documents using time-stamp protocol (TSP) and online control of the public key certificate status at the time of signing [12,19-24]. So, IDS verifies both the authenticity of the signature on an e-document (the signature's owner, the absence of falsification in the document), and the time of signing and the authenticity of the public key certificate during the digital signature. The time stamp is for the verification of the document's existence in a particular time period. This technology is based on the digital signature and hash functions [21]. The time stamp can be considered a digital certificate which guarantees that e-documents existed unaltered until a particular time period and were not modified in subsequent periods.

The issue of key management. When providing information security services, the digital signature (DS) and other cryptographic (symmetric and asymmetric) technologies play a prominent role [3,6]. DS is conducted with public key infrastructure and is based on trust in the public key certificate given by certificate authorities (CA). The public and private keys are generated in asymmetric cryptography. The public key is used for e-signature verification and is open to everyone. The private key is used to create e-signatures and must be known to the signature owner. The keys allow the encrypting and decrypting of information. That is, the information encrypted with a key can be decrypted with a private key only. Because of the large calculations required, it is very hard to find a private key for a public key [3, 12].

A private key is the most sensitive component of digital signature cryptosystems. Malicious parties that have seized the private key of a user can sign any document on behalf of that user. Hence, the signature security is paramount. The security of the private key of a user must be maintained at all stages of its lifecycle: at the generation stage of public and private keys and during the storage, application and liquidation of a private key. The generation of key pairs (public and private) must be conducted in an environment which precludes the probability of malicious parties seizing information concerning a public key to be used during recovery attempts. During the storage of a private key, its privacy and completeness must be protected from modifications without permission. Thus, particular attention must be paid to private key storage.

According to electronic signature law, the storage of private keys is the responsibility of the owner. Users can store the private key in personal computers protected with a password. The security of a public key depends on computer security in general and a user must sign this document on a computer only. Floppy disks, smartcards and USB devices can be used for private key storage. The storage of private keys on smartcards is preferable because a user must possess the card and enter a PIN code to obtain two-factor authentication. In case of the loss or theft of a storage device, the certificate must be recalled. During the use of a private key, it is possible to prevent its seizure and use without permission (by considering the request of a user). Finally, at the liquidation stage of a private key, the probability of its repeated use must be prevented.

Cryptographic hash-functions (*MD5, SHA, RIPEMD*, etc.) must be used for control of completeness. Hash functions calculate hash code for information of a fixed size, and this code is related to information; the hash-code also changes as bytes change [3].

EDMS development must be strongly supported by the state because EDMS plays a prominent role in e-services provided by the e-state. Legal support for EDMS must be closely considered as demand grows for a secure e-document exchange among departments. Juridical novelties in this field boost the development of prospective technologies, enabling the increase of the security of information resources and reducing fraud.

Mobility in EDFS and the application of cloud technologies and threats

The expansion of web services has affected the development of electronic document flow. Reports and forecasts of analytical companies have shown that the application of mobility and cloud technologies are development trends in EDMS [5, 25–27]. Although an EDMS based on Software as a Service (Saas) is not widely applied in business entities, EDMS has become an irreplaceable tool in the accurate management of resources and costs in cloud computing. The development of an EDFS based on an SaaS service model can increase flexibility in the content management sphere by significantly reducing spending on server purchases and software licenses of organizations [25]. All issues in cloud computing concerning information security can be solved with contracts, regulations, agreements and other documents that constitute service level agreements. Naturally, service providers are interested in avoiding violations because their activity is based on trust. An important part of security maintenance is constituted by non-disclosure agreements that provide legal protection of documents and specify the liabilities and disclosure responsibilities of the parties. The access issue for unauthorized users can be addressed with smart control mechanisms, but the cloud is not protected against traditional threats such as document theft, distributed denial of service (DDoS) attacks and service hacks. When malicious parties try to seize the data, they encounter professional program tools of service providers, for example, the *Cisco ASA 5500 Series* and *IronPort* devices. The mistrust problem for an operator can be solved with certification standards used to maintain security, accessibility, the completeness of data processing, and privacy.

The demand for mobility has become a serious threat for EDFS security. Mobility overcomes almost all boundaries of information security, and facilitates new security problems. The emergence of new mobile devices has intensified this problem [26]. The boundaries differentiating a network with public access from private networks, mobile devices and stationary devices, and the division between the employees of an organization and unauthorized users are eliminated. With the expansion of the functions of modern mobile devices, users utilize the data synchronization function between computers and smartphones, making security maintenance more difficult because an employee can use different operating systems, program applications and networks on personal computers at work, on a smartphone while travelling and on a notebook in the hotel. Mobile devices of employees are connected to Wi-Fi and networks beyond the control of their organizations; traditional security mechanisms such as the firewall are not sufficient for system security maintenance during mobile connections. The firewall divides the world into two parts: “white” and “black” or “foreign” and “home”. Current security systems must consider additional factors including network topologies, dynamic attributes (user profile, location, network access) and monitor the users through identification and authentication and rights verification methodologies [23]. This approach requires a large amount of work. With the increase of online information services, large banks and insurance companies may act as parties interested in combatting fraud, and they may assist in the creation of these systems. In general, the protection against information threats is a complex problem. Information security systems must be at the fore front of protection.

Conclusion

The application of EDFS has become a necessary factor in the solution of management tasks in both the private and government sector. EDMS security must be approached as complex, and the threats, risks and losses to be incurred must be correctly evaluated. Weak authentication, the absence of cryptographic tools and the complexity in EDS applications are the factors that preclude an advanced, secure EDMS. This, in turn, impedes the transition from paper documents to e-documents.

EDMS security is not confined to document security and accessibility. The protection of the network environment including system tools and data transfer channels is important. Hence, the implementation of complex security plays a prominent role at all levels, but it is often disregarded. Poor administration may reduce the most modern technical measures to zero.

References

1. Sprague R.H. Electronic document management: challenges and opportunities for Information Systems Managers // MIS Quarterly, 1995, vol.19, no.1, pp.29–49.
2. Hajirahimova M.Sh. Actual problems of electronic document management systems in the framework of electronic government environment and their solution methods // Information society problems, Baku, 2010, №2, pp. 21-29.
3. Aliguliyev R.M., Imamverdiyev Y.N. Digital Signature Technology, Baku, "Elm", 2003, 130 p.
4. Resolution on electronic signature and document of Republic of Azerbaijan, Azerbaycan newspaper, 10 March 2004.
5. Kolesov A. The state and EDFS: conclusions, problems, perspectives. 25 March 2011, Available at: http://ecm-journal.ru/post/
6. Malyuk A.A. Information security: conceptual and methodological foundations of information protection. Moscow, Hot Line Telecom, 2004, 280 p.
7. Lambrinoudakis C., Gritzalis S., Dridi F., Pernul G. Security Requirements for e-Government Services: A Methodological Approach for Developing a Common PKI-based Security Policy // Computer Communications, 2003, vol.26, no.16, pp.1873-1883.
8. Resolution on interdepartmental electronic document flow system, 4 September 2012, Available at: http://www.president.az.
9. Resolution of information, informatization and information security of Republic of Azerbaijan, 3 April 1998. Available at: http://www.president.az.
10. Buldakova T.I., Glazunov B.V., Lyapina N.S. Efficiency assessment of electronic document flow system security // TUSUR Proceedings, 2012, № 1 (25), part 2, pp. 52-56.
11. Dosmuhammedov B.R. The analysis information threats to electronic document flow system // Computer software and computer engineering, 2009, № 6, pp.140–143.
12. Imamverdiyev Y.N., Hajirahimova M.Sh. Infrastructure architecture of trust to electronic documents in electronic state environment // Telecommunications, 2011, № 11, pp.18–26.
13. Riverst R.L., Shamir A., Adleman L. A Metod for Obtaining Digital Signatures and Public-Key Criptosystems // Communications of the ACM.-1978.vol.21, no.2, pp.120-126.
14. Liu J.B., Hu X-Q., et.al. Design and Implementation of a PKI-Based Electronic Documents Protection Management System / Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kaohsiung, Taiwan, 26–28 November, 2007, pp.87-92.
15. ITU-T X.842 Information Technology – Security Techniques – Guidelines for the Use and Management of Trusted Third Party Services, 2000, 50 p.
16. Housley R., Polk W., Ford W., Solo D. RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002, 129 p.
17. Pinkas D., Pope N., Ross J. RFC 5126: CMS Advanced Electronic Signatures (CAdES). 2008, 141 p.

18. Myers M., Ankney R., Malpani A., Galperin S., Adams C., RFC 2560: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP, June 1999, 51 p.
19. Cain A. C., Pinkas P. D., and Zuccherato R. RFC 3161: Internet X. 509 Public Key Infrastructure Time-Stamp Protocol (TSP), august 2001, 26 p.
20. Gatautis R., Mazeika A., Laud P., and Satkauskas R., Enhancing e-Government Services through Digital Time Stamping: Time Stamping System Specifications // Communications of the IBIMA, 2008, vol.5, no.24, pp.204-210.
21. Buldas A., Laur S. Knowledge-binding Commitments with Applications in Time-Stamping / International Conference on Theory and Practice of Public-Key Cryptography (PKC'07), 16-20 April 2007, Beijing, China, LNCS 4450, pp.150-165.
22. Freeman T., Housley R., Malpani A., Cooper D., Polk W. RFC 5055: Server-Based Certificate Validation Protocol (SCVP), December 2007, 88 p.
23. Farrell S., Housley R., Turner S. RFC 5755: An Internet Attribute Certificate Profile for Authorization. January 2010, 50 p.
24. Adams C., Sylvester P., Zolotarev M., and Zuccherato R., RFC 3029: Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols, February 2001, 51p.
25. Liu N. Cloud technology in the security management of enterprise document / Proceedings of the second International Conference on Innovations in Bio-inspired Computing and Applications, 2011, 16–18 December, pp.267-269.
26. Corazon M.G., Sicat E., et.allSubioniPad: Integrated Paperless Document Checking and Template-based / Proceedings of the Second International Conference on Computer and Electrical Engineering, 2009, pp.189-193.
27. The Digital Universe Decade – Are You Ready?,http://www.emc.com/collateral/ analyst-reports