Emerging Research and Solutions in ICT 1(1):68–74 DOI: 10.20544/ERSICT.01.16.P07
UDC: 004.6/.7.056:35.07-049.6

Proposals for Amending the Regulation of the Administrative System

Zoltán Nyikes[1], and András Kerti[2]

[1]Óbuda University/Doctoral School on Safety and Security Sciences, Bécsi str. 96/b, 1034 Budapest, Hungary
nyikes.zoltan@mil.hu
[2]National University of Public Service, Ludovika square 2., 1083 Budapest, Hungay
andras.kerti@uni-nke.hu

Abstract. The paper presents the history of the Middle Hungarian administrative system. This administrative system is operating under the current government regulation and the administration is depicted as an information security element. The paper describes the operation of the administrative order of today's challenges. The electronic administration is a result due to the increasing number of enterprises and public administration sectors. In corelation with this issue suggestions and expected future trends of the administration tasks list are presented. By analyzing the problems that appear during construction of the administration system, possible solutions are presented.

Keywords: information security, electronic information security, administration system, administration security, ASP

1. Introduction

Administration is a complex task which includes the processing of cases and the management of open and classified documents or data in accordance with the relevant legislation. The management of data and documents is performed by means of registration. Therefore, administration is a specific system of processing cases within the organization. It is designed to fulfil the role of an information system which is controlled by the monitoring of feedback in the process. In fact, administration is nothing more than the sum of information processes.

1.1. Administration as a part of information security

Administration fulfils the role of document protection in administrative security, which forms a part of information security. As defined under Act L of 2013 on the

Electronic Information Security of Central and Local Government Agencies [1], administrative security includes the organizational, controlling and regulatory measures taken to ensure protection, and the training procedures related to security.

Administrative security and administration are performed within a regulated framework in Hungary. General administration is regulated by Government Decree No. 335/2005 (XII. 29) on the general requirements for document management set out for the standardized management of public administration [2]. This decree forms the basis for the order of administration in such organizations which deal with general, non-classified information. With respect to national and foreign classified information, Act CLV of 2009 on the Protection of Classified Information and the National Security Authority [3], and Government Decree No. 90/2010 (III. 26) on the management of classified information [4] must be applied.

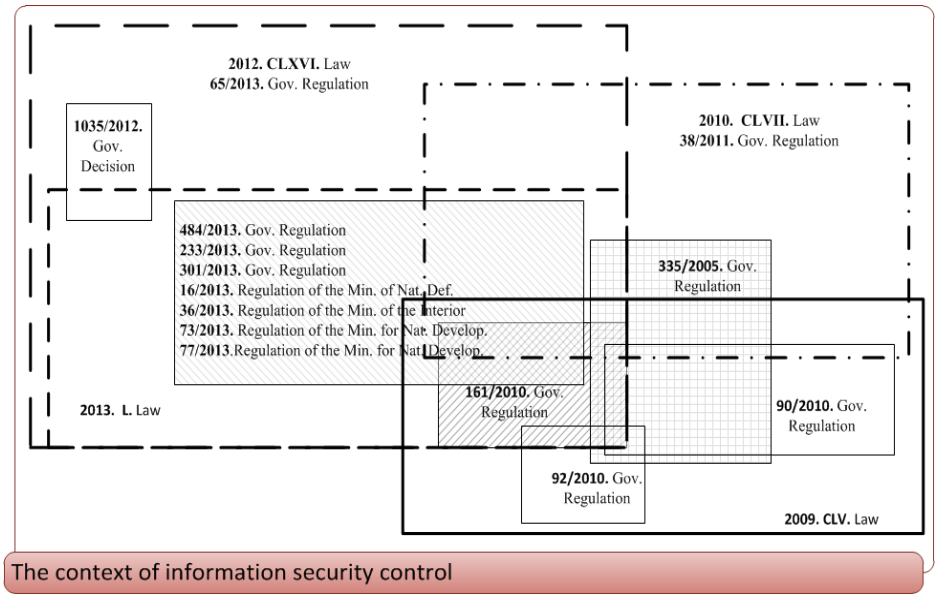

Fig. 1. The context of information security control (by the author)

Interestingly, the European Union and NATO, of which Hungary is a member, set regulations for the protection of classified data only. Such regulations include, for example, the COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU) [5], the COMMISSION DECISION (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission [6], and the SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION (NATO) DOCUMENTUM C-M(2002)49 [7]. The requirements set out in the above regulations are the same as in the national legislation, or, in many cases, the national regulations are more strictly controlling than federal regulators.

2. The current state of administration

Unfortunately, due to these stringent rules, the administration system is often limited to the paper-based management of documents. The regulations controlling national administration could not sufficiently adopt the processes of electronic filing and case management which could ensure the simplicity and speed expected by the knowledge-based or information society. Legislators see the paper-based management of printed documents as a guarantee for security in administration. This leads to two assumptions. Namely, it might be that legislators only carried out preparatory work in a very restricted circle with the exclusion of the representatives of the security industry. They did not take into account the speed of technological progress and the demands of the society, but only aimed to maintain their dogmatic principles. Or, these legislations were prepared by a professional body which thoroughly examined the potential technological advances and their security risks. However, having taken these considerations into account, they came to the conclusion that the current level of technological development does not allow electronic administration to replace the paper-based administration of printed documents. The potentials of electronic administration are not sufficiently exploited because of this rigorous legislation. Electronic administration and the systems of organizational administration are regarded as a kind of transitory option. Certainly, it is a fact that the electronic form of information is one of the most vulnerable and most compromisable forms. However, electronic information security experts are constantly working on this issue to make this field safer from the point of controls and technical conditions. This is reflected in the fact that the federal regulatory system is less stringent than the national. As a consequence, federal regulators allow for electronic administration in the case of classified and non-classified data.

2.1. The current use of the electronic administration system

Naturally, administration, as a part of information security, shows some progress in the field of IT applications. Legislators have made a number of amendments to the abovementioned Decree No. 335/2005, and one of these amendments has opened the possibility of electronic administration. One of these amendments is Government Decree No. 62/2015 (III. 24.) on the ASP centres of municipalities [8]. This Decree allows the possibility for municipalities to use an information system providing remote application service through the Application Service Provider (hereinafter: ASP) infocommunication network ensured by the Hungarian Treasury and the National Infocommunication Service Ltd., one module of which is electronic administration.

2.2. What is ASP?

ASP, or application service provider, refers to a new business and technological construction. Within the framework of ASP, the users access management or other software products which are necessary to support their activities by connecting to the servers located at the service provider and using databases and other data management programs through the Internet. Therefore, it is enough to run a simple web browser on the users' computers with Internet connection.

In case of ASP, the user access a software application together with the related hardware and operational services. This way the user can perform his daily management and administration tasks himself. All other related tasks, such as data storage, data backup, software updates, and application, as well as the operation and maintenance of the server infrastructure is outsourced [9].

2.3. Document Management System

The Document Manager Application allows the implementation of a uniform, transparent document management system both in its methods and on the level of IT support. It enables the entire range of document management, from receipt to scrapping. It covers the document management activities and the implementation of a centralized, distributed or mixed document management system in each organizational unit. It helps to process large amounts of data and provide an opportunity to implement paperless administration. Managers can sign documents, define document management tasks or deadlines, track the progress of implementation, and exert control over the system on their own computers [10].

3. The appropriateness of regulation

As discussed in the preceding paragraphs, in the areas of information security control laws, government regulations and ministerial decrees, the aim of all that information security should be guaranteed. However, as IT equipment for the production and transmission of information, amortization and obsolescence approach is quite high, guaranteeing the security of obsolescence controllers is high as well. Therefore, the existing regulators control and modification is required. The continuous change and move towards effective protection requires that the currently case-reviewed controls be carried out and their number is reduced by the creator of the legislation.

3.1. The regulations for the protection of classified data update

Several controllers, mentioned before, regulate the same area. On the other hand, if they are merged, that would greatly help the applicability and thereby the security of information. Such example is the previously mentioned operation of the National Security Authority, as well as the operation of the order dealing with classified data decision 90/2010 (III. 26) Government regulation [4] and the security of electronic data, as well as certified crypto activity for approval and official supervision of the detailed rules of 161/2010 (V. 6) Government regulation [11]. The structure of the two terms of the same Decree. In some cases, practically 90/2010 Government decree – a supplement to the 161/2010 Government decree. If these lines would be reviewing government regulations forming part of the legislation, which is timely, in that case it would be the proposed merger of two government regulation of content and changes that took place in the identified gaps.

However, not only how the protection and its regulation, but also to the creation of classified data is also necessary to review the procedure laid down for it. In conclusion I Reasons to that of the current Act CLV of 2009 on the Protection of Classified Information [3] in particular in the preparation of the law on the control of paper-based classified data protection was the main goal. However, decades earlier was proven that the information is not only a piece of paper that can be stored and transmitted in written form, but also in electronic form, which can be analog or digital, too. The electronically stored and transmitted classified data, currently the administrative register of regulations, is nothing more than a paper-based administrative rules "abuses" in the form of "new" appearance. This construction is workable as long as it did not reveal the demand for electronic transmission of classified material. Currently this is the point the Hungarian control cannot get past, and information security professionals are looking for a solution. Actually, the solution is before our eyes, because NATO's electronic classified data transmission to the federal system (email) system, effectively for many years, transmits classified material by electronic means.

3.2. The anomaly of the electronic transmission of the national classified material

The the problem of the national electronic transmission of classified material, due to the legislature that hold to the old dogmatic principles, practices, and that the information can only be classified by certain people or classified information are created, if the law has specified formal accessories. In contrast, in the electronic system used in NATO, a person who has access to the system, under the conditions of personal security, can send letter which contains classified information to any user in the system, with a requirement to select a letter and attach it to the certification level. From that point on, the sender and receiver is required for the level of protection provided for, in the specific certification rules to deal with the substance.

But, the transmission of classified material includes more problems. Currently the NATO procedure described above does not apply to the national order of classified material. Although the technical conditions under which the electronic transmission of the national classified material are fulfilled, the national regulators does not allow it. National data only in the law, and the various policies requires qualifying a person as well as the formal properties (such as a certification date and sign of the person's certification clause), without which there can be no classified data. The certified electronic signature, known as the PKI[1] system, could be triggered.

However, this solution of the Hungarian public administration is in the testing phase (performing tests transmission). The establishment of the system, is extremely important. The disadvantage of this solution is that it does not resolve the anomaly that a person presents, solely because it cannot "get rid of" the use of classified information in the formal accessories.

3.3. The administration anomaly of the national electronic classified information

Other obstructions in relation to electronic transmission of classified information, is the registration number by the machine, called application of the RNM[2]. This is no different than the registered certification marking and electronic media, such as hard disk - HDD[3] (i.e. the registration number of the Interleave, which is the same as the number of HDD recording – and produced number of the current record sequence number). Using the RNM for the electronically produced data, which contains information that is classified, is a starting preparation that ensures the traceability of the data, or the guarantees that they will provide nonrepudiation. The Interleave is documented in the exact description of the data stored, the file ID, path, the time of construction, delete and overwrite; and at the time of printing, the number of printed pages, number of pages, spoiled the fair copy of receipt date and signature. On this basis, it can be seen that the data has been classified in the communication, and can be kept track of the Interleave on the basis of the RNM. This registration system does not classify the data and it will be registered only until after it have some kind of ID for monitoring, which is based on the classified data in order to track life of the document.

In addition, in the case of data transmission as well as network storage server this solution is not suported. This registration option only works with stand-alone computers. In the Central Server the use of the RNM private cloud is nonsense, because the path for the user will not be published. So this is solution outdated and has picked up the "retirement" of the time.

---

[1] Public Key Infrastructure

[2] Registration Number by the Machine (Hungarian name is Gépi Nyilvántartási Szám - GNYSZ)

[3] Hard Disk Drive

In printing, NATO uses administration and registration of data to track the ID signal called “Number of the Print Log”. This ID is used by NATO as a proof print of the administration before the registration.

This solution also serves on the trail, but is significantly simpler solution and supports the work of certified network. The system guarantees the traceability of certified comprehensive logging system, which can be traced back to the classified material who, when, where, and what kind of access or changes he or she has made.

4. Summary

In the paper were presented some Hungarian public administration system problems. The administration system position and role of information security as part of administrative security were disscussed. The paper introduces the legislation, which operates on the basis of the national administration system, as well as NATO and the European Union's administrative security. Proposed solutions, based on the analysis of the problems, is presented. The question of the analysis was why not to apply IT solutions in paper-based administration system. The application of the analyzed solution provides administration system with paperless office and paper-based administration. This system is more secure, not only for the public sector but also in economic life. Finally, proposed amendmans of the administrative control will assist and facilitate the electronic transmission of sensitive documents.

References

1. Act L of 2013 on the Electronic Information Security of Central and Local Government Agencies
2. Government Decree No. 335/2005 (XII. 29) on the general requirements for document management set out for the standardized management of public administration
3. Act CLV of 2009 on the Protection of Classified Information
4. Government Decree No. 90/2010 (III. 26) on the management of classified information and the National Security Authority
5. COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU)
6. COMMISSION DECISION (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission
7. SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANISATION (NATO) DOCUMENTUM C-M(2002)49
8. Government Decree No. 62/2015 (III. 24.) on the ASP centres of municipalities
9. Zalaszám ASP központ, Mi az ASP?; http://www.asp-kozpont.hu/mi_az_asp.php; download: 5 Nov 2015
10. Zalaszám ASP központ, Iratkezelő rendszer; http://www.asp-kozpont.hu/organi.php; download: 5 Nov 2015
11. Government Decree No. 161/2010 (V. 6) the security of electronic data, as well as certified crypto activity for approval and official supervision of the detailed rules