HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

**Kovács Zoltán**
zkovacs@nbsz.gov.hu

# „ELECTRONIC WRITTEN TASKING ORDER SYSTEM" ACCOMPLISHED WITHIN THE PROJECT „SECURE ELECTRONIC COMMUNICATION" I.

### *Abstract*

*The "Comprehensive Programme for Integrated Governmental Functions" includes such relevant national security developments as the project named "Secure Electronic Communication" initiated by the Special Service for National Security (SSNS). The so called "Electronic Written Tasking Order System" was accomplished within the framework of this project. The main objective of this system is to convey the written tasking orders sent to SSNS via secure electronic communication lines decreasing the quantity of the paper based data carriers, which results rapid fulfilment of the requests of the tasking organizations, as well as it creates opportunities to carry out several related procedures in electronic form. This article series describe the designation of the Electronic Written Tasking Order System through the activities of SSNS proving that this system is a cloud system in terms of the tasking organizations.*

*Az „Integrált kormányzati funkciók átfogó program" olyan nemzetbiztonságilag fontos fejlesztéseket is tartalmaz, mint például a Nemzetbiztonsági Szakszolgálat által kezdeményezett „Biztonságos elektronikus összeköttetés" tárgyú projekt. Ennek keretén belül került sor az un. elektronikus Szolgálati Jegy Rendszer megvalósítására, amelynek fő célja a szolgálathoz beérkező megrendelések biztonságos elektronikus úton történő továbbítása, ezáltal a papír alapú adathordozók számának jelentős csökkentése és a megrendelői igények mihamarabbi kiszolgálása, valamint bizonyos kapcsolódó ügymenetek elektronikus alapokra helyezésének megteremtése. A cikksorozat a Nemzetbiztonsági Szakszolgálat feladatain keresztül bemutatja az elektronikus Szolgálati Jegy Rendszer rendeltetését, majd bizonyítja, hogy az a megrendelők szempontjából felhő alapú rendszernek tekinthető.*

***Keywords:*** *electronic tasking order system, cloud computing, cloud security, critical information infrastructure ~ elektronikus Szolgálati Jegy Rendszer, felhő alapú rendszerek, felhő alapú rendszerek biztonsága, kritikus információs infrastruktúra*

## INTRODUCTION

The following paragraph can be read in a study published in 2010, entitled: "Computer Network Operations: Threats and Possible Defence Solutions in Hungary"

*"The "Comprehensive Programme for Integrated Governmental Functions" includes such important issues related to economy and national security that we cannot disregard. By means of the "Central Management System" the whole budget system of Hungary will become transparent, therefore misuse of data gained from this system might influence the whole economy of Hungary. Thus the protection of this system is a high priority. The "Taxpayer-centric data service model" sets up Data Warehouses, here the priority is to maintain tax secrecy. The "Secure Electronic Communication" affects the processes of the Special Service for National Security. Although this is one of the most interesting tasks, its technology is not known to the public. The budget of the whole programme is 13881 million Forints."* [1]

If the author of this part of the study, Csaba Krasznay regarded the project named "Secure Electronic Communication" as one of the most interesting issues, it is worth examining what it means. Certainly, only those parts can be published which do not contain classified information, even though the principle of the above mentioned project can be known, with some other important pieces of information which can be necessary for the planning of other systems.

The first article of this series of articles reviews the designation of Electronic Written Tasking Order System (eWTOS) accomplished within the framework of the so-called "Secure Electronic Communication" project, and in accordance with the tasks of the Special Service for National Security (SSNS), the procedure of the orders, and then examines how the eWTOS can be applied in the IT strategy of the Ministry of Interior. The second article analyses a currently important issue proving that the eWTOS can be regarded as cloud computing in terms of the tasking organizations that send written tasking orders to the SSNS. Concerning this it groups the cloud computing along with their features and classifies the eWTOS in the appropriate category. The third article discusses the security issues of the cloud computing by analysing to what extent it concerns the eWTOS as well as how the security panels prevail during their accomplishment. Finally two conclusions are drawn. On the one hand, even though the eWTOS has not been qualified as a critical information infrastructure yet, as every condition is given it is only a question of time. On the other hand, thanks to the already evolved high level security panels, the system is protected properly, thus after the classification these do not have to be modified in merits.

The series of articles concentrate on – primarily security – solutions considered during the planning. These articles do not aim to analyse the technical or other problems which appeared during the implementation or to describe different mistakes and their handling. They will only be mentioned if it is necessary to explicate the previously mentioned issues.

## THE DESIGNATION OF EWTOS

In order to understand the purpose and the functions of eWTOS, first we should clarify the tasks and the procedure of the services requested from the Special Service for National Security.

### Responsibilities and Activities of the Special Service for National Security

Act No. CXXV of 1995. [2] entered into force in 1996 and the SSNS was separated from the National Security Office and it was established as an independent organization with special technical and operational capacities.

SSNS is a governmental agency with nationwide authority, which functions as an independent budgetary organization, however, it is not a traditional national secret service. According to the Act No. CXXV of 1995 it provides the special means and methods of covert information gathering and acquisition of data, but does not have independent intelligence, counterintelligence or investigative powers (except cases concerning the internal security). It uses special means and methods in order to carry out the requests of other organisations authorised by law to initiate and perform covert information gathering (tasking organisations).

After the multiple conversions of the tasking organization structure, currently the SSNS provides special means and methods of information gathering for the reconnaissance and investigative tasks for eight organizations:

- Constitution Protection Office
- Information Office
- Military National Security Service
- Counter Terrorism Centre
- National Police
- Service for Protection of Law Enforcement Agencies
- National Tax and Customs Administration of Hungary
- Prosecution Service of Hungary

With its criminal investigation supporting task-system the activities of SSNS goes beyond the sphere of national security, what is more, supporting these tasks, though indirectly, it is concerned in the execution of cases related to cross border criminal investigation tasks (e.g. organized crime, illegal migration) as well. The SSNS with its capacities of special means and methods has always had a great role in the reconnaissance of serious crimes and events occurring in Hungary emphasized from national security aspect.

So the basic function of SSNS is to provide operational and technical background for information gathering, acquisition of data, as well as expert services for organizations authorized by law with its special technical background and well trained personnel– within the framework of law. It should also be emphasized that the capacities of SSNS do not substitute the traditional national security and investigative work, but significantly increase the effectiveness of those activities.

The concentration of the capacities of information gathering and acquisition of data at the SSNS has professional and economic advantages, as well as provides legal guarantee.

Economic advantages:

- the budget sources are not fragmented,
- the responsibilities and the expenses related to the operation, maintenance and development are concentrated at one organization, the SSNS,
- all of the tasking organizations gain the advantages of the development.

Professional advantages:

- concentrated development adapted to the requests of the tasking organizations,
- nationwide coverage,
- non-stop availability, reacting to the requests immediately, meeting the requirements of the tasking organisations
- coordination ability in case of authority conflicts,
- the elimination of the danger of disclosure caused by equipment applications realized through different principles.

Legal guarantees:

- SSNS cannot dispose with the information gained, it is deleted from its records without reproduction,
- there is no opportunity for “stocking” data acquisition,
- the separation of the tasking organizations and executors strengthens the social trust,
- as an independent service organization the application of special means and methods differing from the content of the external authorization in another way than described in the authorisation is not permitted.

The SSNS – in accordance with the rules of law - has exclusive powers related to those segments of special means and methods of covert information gathering and acquisition of data subject to external authorization where the developing of complex, technical systems requiring significant financial investments, special skills and experience, as well as the existence of human resources possessing special skills (such as off-air intercept, postal censorship) are required. On the other hand, SSNS plays a major role in other fields, for example wiretapping, radio monitoring, physical surveillance and background check.

The Special Service for National Security runs an Institute for Expert Services, which is primarily responsible for providing expert opinions in the field of handwriting, linguistics, audio, photo-video, IT, document forgery and explosives. It also performs regulatory, authoritative, and expert functions. It defines the security specifications for and regulates and supervises the production of the so called security documents. SSNS plays a similar role in the field of securities (shares, stocks, bonds) and authorizes their issuance and controls their production.

The SSNS provides combined application of several services (complex execution) for the tasking organizations, thus with the exploitation of synergy the efficiency can be increased significantly.

In order to protect the personal data and the special means and methods of covert information gathering, all data obtained in the course of covert information gathering is transmitted to the tasking organizations in a documented form and then in accordance with the rules of law they are deleted from its record. The SSNS keeps a record including:

- the request of the tasking organization with the necessary authorization,
- the personal data required for the identification of the person named in the request,
- the description of the special means and methods applied in the given case, and
- the list of data carriers transmitted to the tasking organization.

## The Procedure of Written Tasking Orders

The tasking organization is responsible for obtaining the external authorization or for the issuance of the internal authorization and for the legality of such authorizations. SSNS is responsible for the competent application of the means and methods of covert information gathering and acquisition of data.

The special means and methods of information gathering can be required from the SSNS in written form on unified written requests signed by leaders of high rank whose positions are defined by cooperation agreements. The services of SSNS, where unified written tasking orders are not adapted can be requested through written requests in letter form. The tasking order requesting the application of the special means and methods of information gathering subject to external authorization must be attached to an authorization signed by the Minister of Public Administration and Justice or a designated judge. In case of private requests the description of the task must also be attached.

The procedure of written tasking orders of covert information gathering requiring authorization by the designated judge or the Minister of Public Administration and Justice is shown in Figure 1.

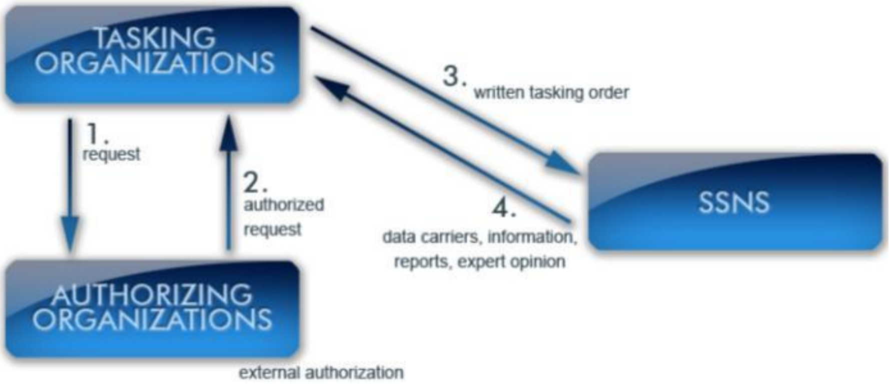

**Figure 1.** The Procedure of Written Tasking Orders

Source: http://www.nbsz.gov.hu/main.php?l=hu&p=1&a=7, (downloaded: 16/03/13)

From 2006 approximately 70,000 orders are obtained from the tasking organizations annually, which means 250, 000 sheets of paper with the supplementary documents every year.

## The Functions of eWTOS and the Milestones of its History

The idea of Electronic Written Tasking Order System – i.e. fast and safe transmission of the written tasking orders and the supplementary documents to the SSNS – was the idea of the IT experts of SSNS in 2005. The SSNS negotiated about the main details and the previous cost estimates with the Ministry of Interior that year and with the other tasking organizations the following year. The project was first set in the action plan of National Development Agency (NDA) in Electronic Administration Operational Programme (EAOP) 2007-2008, and then based on the government decree 2142/2007. (VII.27.) [3] as an emphasized project in the 2007-2008 action plan under the title “The Structuring of Secure Electronic Communication”. The tender was submitted at the end of 2007 and in the spring of 2008 the Grant Agreement was signed with the NDA.

What caused great changes in the project was the Act No. CLV of 2009 on the protection of classified information (PoCI) [4] accepted by the parliament on 14 December 2009. It fundamentally changed the classification of data, the handling of the classified data, the authorization of systems for handling and the regulations regarding the physical environment.

After the reconsideration of the project two important decisions were made. Firstly, the system will allow the handling of maximum Confidential! level documents instead of TOP SECRET!. This decision results that the documents classified above the level Confidential! will still be obtained in paper form, in exchange the costs of evolving a system suitable for TOP SECRET! level regulations (e.g. reconstruction of buildings) decreased significantly. According to the frames given by the PoCI the amount of documents classified maximum Confidential! will expectedly cover more than 85% of the written tasking orders and other supplementary documents, thus an absolutely acceptable and rational decision was made. The other important decision was that the deadline of the project and the launching of eWTOS were amended to 31 December 2011 which was necessary to perform the new requirement and authorization system defined in PoCI.

In the summer of 2011 a final decision was made which determined that the document handling system of the eWTOS will be the so called “RoboCop” (RC). The background of this decision is the unification of document handling systems used in the bodies of the Ministry of Interior. The adjustment of RC to the eWTOS, the difficulties about the new encryption equipment (debuting in eWTOS), and the other issues which occurred related to reconstruction of the buildings – because of PoCI – and further technical reasons held back the launching of the eWTOS.

Because of the reasons mentioned above the deadline of the Grant Agreement was modified several times after signing in 2008, finally the system has been operating since 1 January 2013.

The function of the Electronic Written Tasking Order System, which was created within the project called “The Building of Secure Electronic Communication” is to transmit (mostly classified) written tasking orders and other supplementary documents (e.g. authorizations) from the tasking organizations to the Special Service for National Security in a secure electronic way instead of paper form. This will result a decrease in the amount of paper-based data carriers (written tasking orders, authorizations) and thanks to the online connection a faster fulfilment of the requests of the tasking organizations. According to the commitments of the project this means that the time of obtainment of the necessary documents from the tasking organizations decreases from 42 hours to 3, the number of paper based documents decreases from 250,000 to 25,000.

The complete electronization currently is not possible because of three reasons. One is that after negotiating with the tasking organizations 157 online terminals were installed which do not cover all the organizations issuing written tasking orders. The second is that the eWTOS handles only Confidential! level documents, thus the documents of higher classification are still obtained in paper form. The third reason is that in case of breakdown or VIS MAJOR (e.g. online terminal outages) the written tasking orders can be obtained in paper form.

The eWTOS has additional advantages besides the commitments. As a result of the two-way connection the system enables the reports to be transmitted to the tasking organization in an electronic form, in a secure way, as well as to lay the relating procedures on electronic basis. This – besides the acceleration of the previously mentioned procedures – results further paper savings in the long run, which was not mentioned in the project.

## The Structure of eWTOS

In the eWTOS three different parties are named as follows:

1. Tasking organizations:
   - the previously mentioned eight bodies.

2. Authorising Organizations:
   - Minister of Public Administration and Justice,
   - the judges designated by the Budapest Metropolitan Court Criminal Department Military Panel,
   - the judges designated by the chairman of Budapest Metropolitan Court,
   - Public Prosecutor.

3. Provider:
   - Special Service for National Security (SSNS).

The principle of operation of the eWTOS is shown in Figure 2.

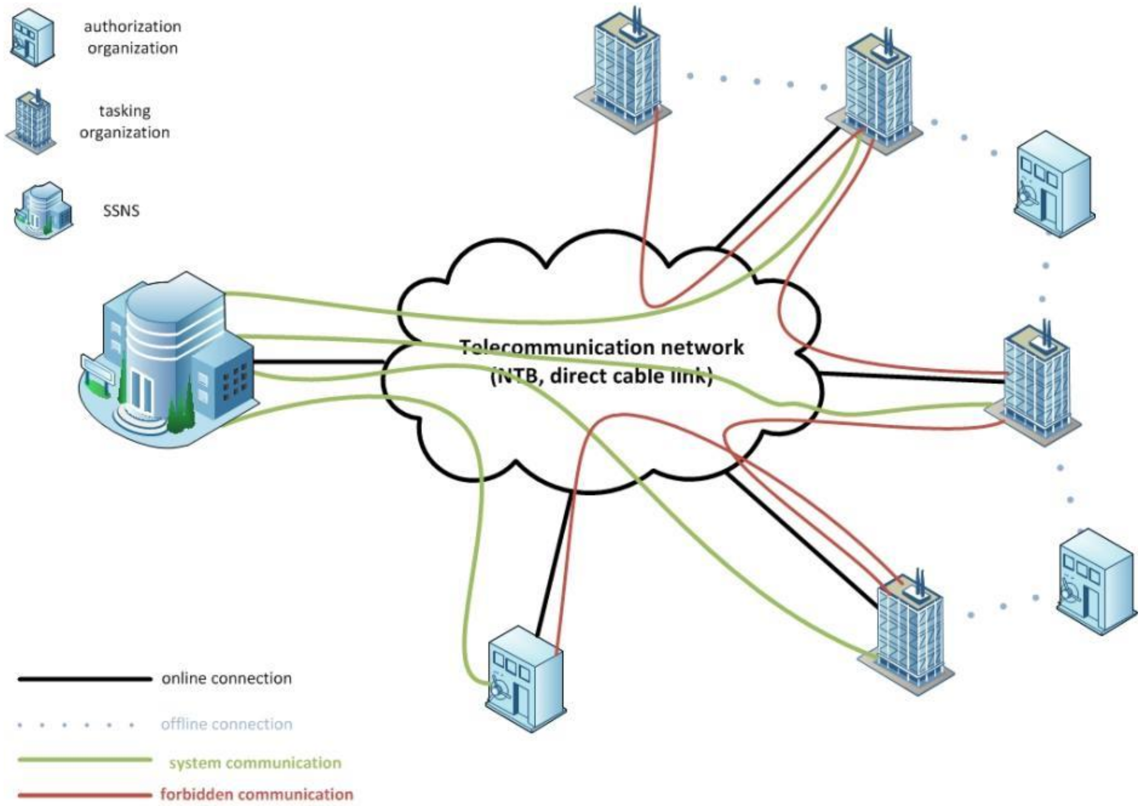

**Figure 2.** The Principle of eWTOS
Source: edited by the author

The figure shows that the tasking organizations are in connection with the devices installed at the SSNS. They send the written tasking orders here and receive the reports from here (Figure 1, Process 3 and 4). The system was constructed for a definite purpose, therefore the tasking organizations have no opportunity to share information different from the original purpose of the project. On the other hand, eWTOS provides the transmission of requests between the tasking organizations and authorising organizations (Figure 1, Process 1 and 2), but in this case the system installed at the SSNS works as an unavoidable quasi-mailbox. (Owing to the encryption and other guarantee elements everyone can only see their own documents, thus these documents are not available even to the personnel of the SSNS before the official transmission!)

The documents can be prepared and transmitted by means of the so-called online and offline terminals. The online work stations are connected to the SSNS centre through a telecommunication network (called National Telecommunication Backbone (NTB) or direct cable connection). In this case all the hardware devices are provided by the SSNS (except the SMART card necessary for the identification).

The structure of online terminals is shown in Figure 3.

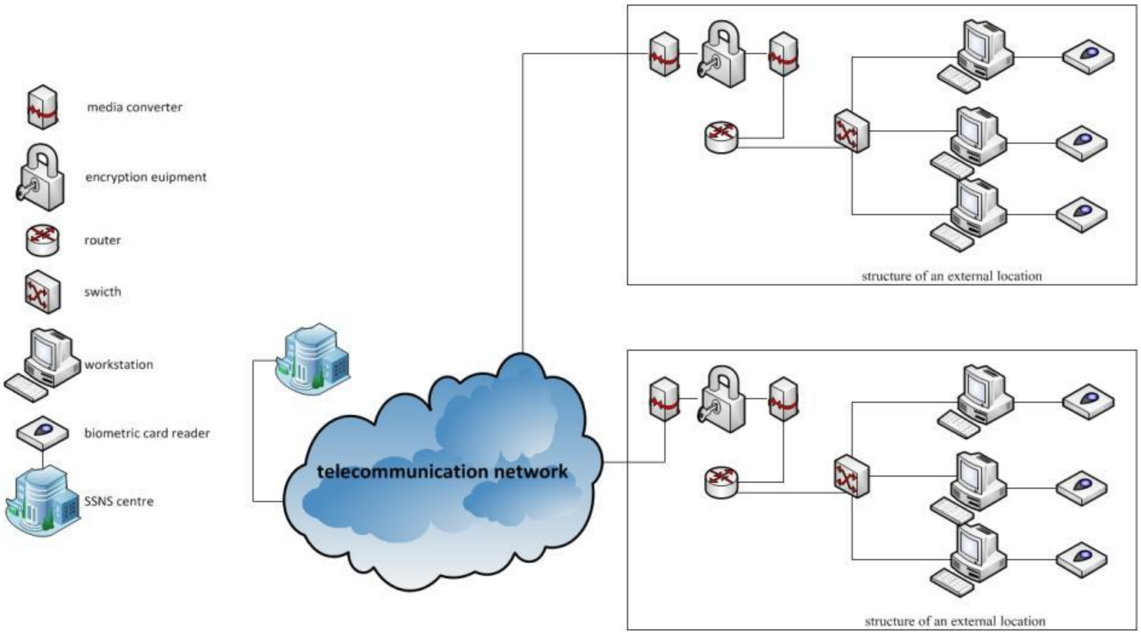
media converter
encryption euipment
router
swicth
workstation
biometric card reader
SSNS centre
telecommunication network
structure of an external location
structure of an external location

**Figure 3.** The Structure of Online Terminal
Source: edited by the author

In case of offline work stations the SSNS provides only an installation kit (since the application of eWTOS is bound to license). In this case the users utilize their own hardware infrastructure and card reader to make and send written tasking orders and other supplementary documents. However, these work stations are not in direct connection with the centre at SSNS. The documents made in offline work stations can be transmitted to the SSNS on data carriers (e.g. CD, flash drive) or through an online work station.

The offline clients can be installed to any suitable work stations, but the protection of classified information has to be provided to avoid unauthorized access and in case of transmission through the online work station it has to be compliant to other security regulations as well (e.g. authorisation of the use of flash drive based on unique identification).

For the operation and use of eWTOS the further devices (e.g. servers, other telecommunication devices etc.) are provided by the SSNS.

For the easier introduction and instruction the purpose of the developers was to replicate the paper-based processes known by the users in the best way possible However, certain changes in the process were unavoidable. These can be followed in the figure below (the workflow of paper-based process is shown in Figure 4, the electronic in Figure 5), where the position of the (system of) SSNS is the most remarkable in the chain.

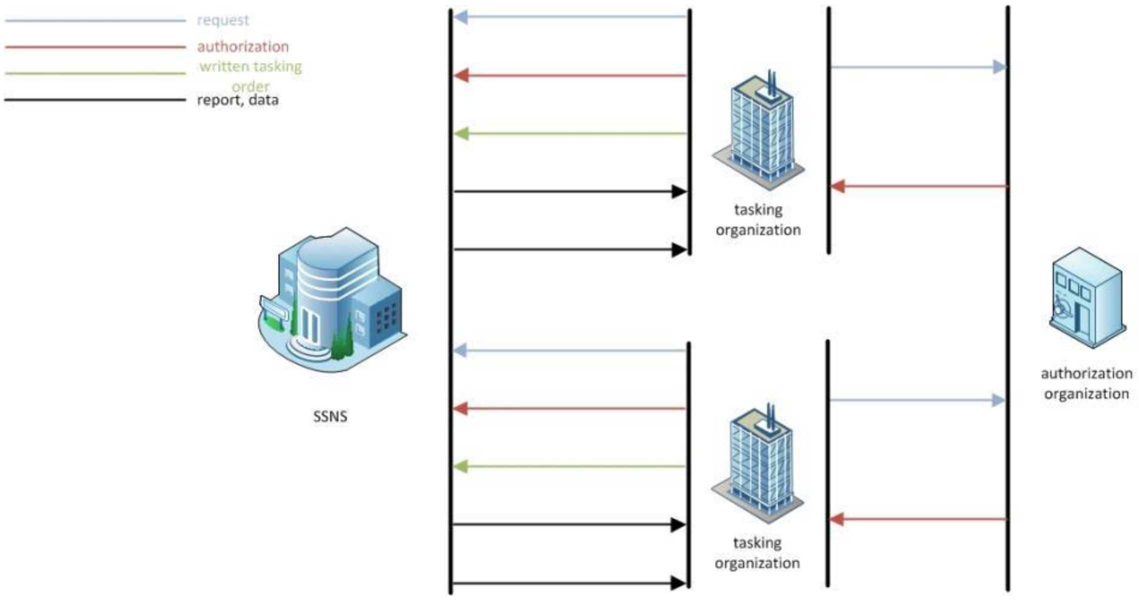

**Figure 4.** Workflow of Paper-based Process
Source: edited by the author

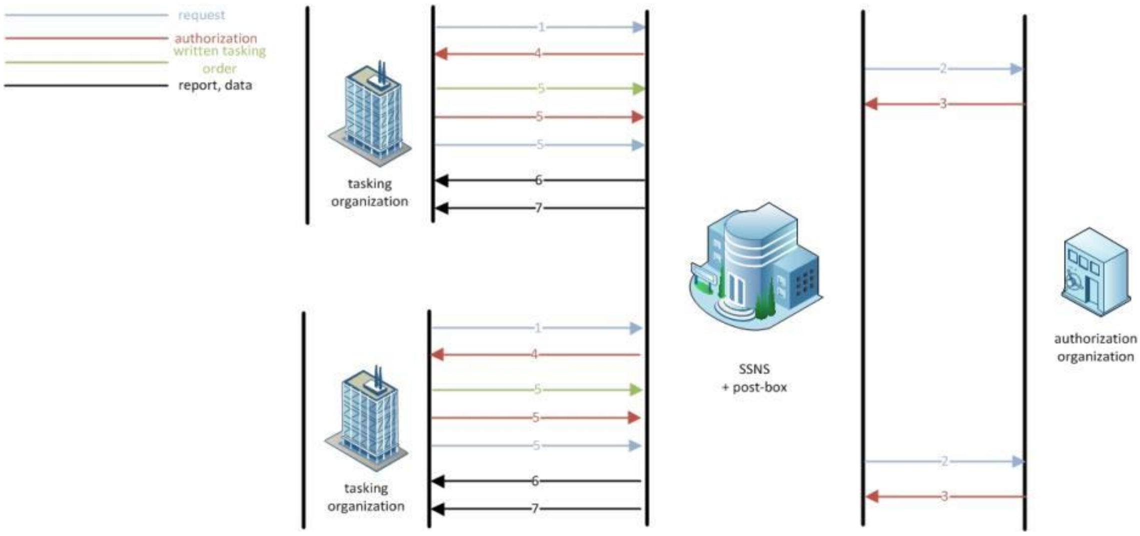

**Figure 5.** Workflow of Electronic-based Process
Source: edited by the author

However, this is not the only essential change resulted by the introduction of eWTOS. The main changes are as follows:

- the electronic files are transmitted,
- the electronic files are more detailed than the paper-based ones,
- the electronic files can only be opened with an application developed by the SSNS,
- the issuance and classification of documents are provided with a digital signature,
- the documents are certified digitally,
- the documents are classified digitally,
- The samples of handwriting signatures can be abolished,
- the handling of copies and appendices change,
- new documents are introduced.

## The Adaptation of eWTOS in the IT Strategy of the Ministry of Interior

The idea of the eWTOS in 2005 was very promising as it suits to the IT strategy of the Ministry of Interior published in 2012(!). [5] As the decree includes the Ministry of Interior and its sectoral organizations, it covers the half of the tasking organizations of the SSNS (regarding the amount of the written tasking orders, this proportion is much higher).

Those parts will be highlighted below from the document mentioned above which justify the fit.

*"III. Strategic methodology*

*2. The rolling wave planning*

- The homogenization of IT systems on sectoral level is required in favour of cost-effectiveness, easier operation, and the use of knowledge base in the sector.
- The different levels of development and security should be approximated on sectoral level.
- Suitable for the legal frames, paper-free administration has to be evolved and the whole electronization of expert systems with customer service has to be evolved in favour of the establishment of an electronic, paper-free office [the introduction of RC NEO integrated management, case processing and electronic record management (hereinafter: RC NEO system)]
- The continuous increase in the level of IT security regulations and environment."

The terminals of eWTOS placed at the tasking organizations, the software on those terminals, document handling systems connected to it (in this case the RC), and the installed security devices (for handling of classified data, authorised encrypting devices and electronic systems, and the use of other security elements) are in the service of unification, approximation of development levels and strengthening and increasing security. The eWTOS itself will replace a part of paper-based processes, thus helping the development of a paper-free office.

The next step of this process is the expansion of RC document handling system on the side of the tasking organizations and SSNS, which will also make some parts of the process paper-free. Let us take a short digression into the future. About the development of RC the following issues can be found in the strategy:

*"IV. Directions of Strategic Development*

*7. The Development of RoboCop System and the Implementation of RC Neo in the Sectors*

*...According to the directions of the Minister of 24 June 2011 a further development of RoboCop was prescribed on new technological basis within the frames of RoboCop NOVA project. In accordance with the decision, the RoboCop should be upgraded based on the current solutions so that it will be suitable for the claims of the new technology, legal background and the average professional standards in the long run preserving the outstanding values of the previous system. In addition, the purpose of the project is to define the regulations and standards which provide the unified technical, semantic, IT security, application development, methodological and project management and to control the environment providing the complete development, maintenance and operation of RoboCop. The realization and consistent enforcement of these purposes provide a guarantee for a RoboCop of excellent quality, based on firm technology and can be utilized in a modern user environment in the long run.*

*During the development the main objective is to emphasize the organizational and user requirements based on legal commitments, special sectoral expectations and operation more efficient than the market structure. The newly developed RoboCop – just like the current* *system dependent on the intended targets - is needed to be audited in favor of the successful certification. A particular emphasis should be laid on the audit from the point of view of security…*

*”The interior sector develops RC, as a management and document processing system from its own resources which satisfies the professional claim in the short, medium and long run. The introduction of RC Neo in the sector was ordered by the Decree of 24/2011 (IX. 9.) of the Ministry of Interior on the regulation of the use of the integrated management and case processing system of RoboCop and on the introduction of unified electronic document management and the establishment of project organization supporting the implementation. After testing the system the management, the case processing and the electronic document management are allowed to be done according to the instructions.”*

So the RC will be the determinative document handling system in the Ministry of Interior and its sectoral organizations in the long run. After its upgrading the RoboCop along with eWTOS will be able to provide a secure, paper-free management between the SSNS and its (RC using) tasking organizations even in the entire process of the case (i.e. from the phases preceding the preparation of the written tasking orders to the activities after the process of the reports made at the Special Service for National Security).

In the eWTOS, as a system handling and transmitting classified data, the security issues have a highlighted role. In the IT strategy of the Ministry of Interior the following statements can be found regarding the eWTOS:

*“8. IT Security*

*Regarding the philosophy of the IT Security Policy of the Ministry of Interior, in the field of IT security sectoral level, centralized purposes have to be followed. To the harmonization of the IT security levels the purposes have to be performed are as follows:*

*...– For the protection of communication of non-public data among the Ministry of Interior and its sectors at least IPSec encryption has to be used. Stronger, higher-level protection can only be used in task orientated, justified cases. ...*

*...– The Ministry of Interior and its sectoral organizations… have to define the borders of their IT network, within which they have to provide all IT protection themselves. In order to guarantee the security of the data stored and transmitted in the network of the organization homogeneously solid network protection devices and defence procedures must be applied.…*

*...In favour of the protection of the IT network of the Ministry of Interior and its sectoral organizations ... keeping a record of the access to the IT network, ... as well as the logging of the printing process.*

*In the Ministry of Interior and its sectoral organizations the following IT security conditions have to be established in favour of protecting non-public information:*

*– The use of not registered mobile data store devices without unique identification has to be abolished. ...*

*– All documents in the electronic document handling procedure must be provided with digital signature and timestamp by their issuers until 31 December 2014.”*

As the eWTOS is a system transmitting classified information the transmission of data require authorised national encrypting devices. The access and the protection of data stored and transmitted in the system are guaranteed by a multiple level protection, authorised devices and sites. The access processes and the printing are provided with high level protection, and completely logged. Only previously registered devices with unique identification can be connected, the events are completely logged in this case as well.

The eWTOS is already accomplishing the security element (the provision of the document with digital signature and timestamp) described in Chapter 8 in the IT strategy of the Ministry of Interior, which is not provided by any other IT systems of the Ministry of Interior, only mentioned as a medium term goal.

Finally, regarding encryption the strategy aims at the following purposes, which are accomplished by the eWTOS as well.

*"9. Encryption*

*The Act No. CLV. of 2009 on the protection of classified information re-regulated all the aspects of the handling of national classified data with the attendance in international communities in Hungary. The purpose of the strategy of the Ministry of Interior on sectoral levels is: ...*

*– The establishment of uniformly high level encryption equipment parks.*

*– The execution of the transmission of classified data in a unified network."*

## CONCLUSIONS

As a conclusion it can be ascertained, that eWTOS outrivalled its time when it was invented. The basic conception was the electronization of a part of a completely paper based process of written tasking orders sent to the SSNS. Apart from the fact that it was a daring, favourable idea, it also had other advantages. On the one hand, eWTOS did not want to electronize the complete process, only its most critical part in terms of investment. It aimed at the field, where the endpoint terminals were installed in more than one organization, the communication lines between these terminals were used in common, that is why it was complicated to share the expenses in a fair way. Moreover the accomplishment of this part of the process could accelerate the electronization of the entire procedure. On the other hand, the implementation of eWTOS in this form enabled the tasking organizations to accomplish their electronic document handling processes concerning eWTOS using methods and equipment they wish. In addition they could do it considering their financial circumstances and developing priorities. Thirdly eWTOS includes such technical solutions and functions today, which were described as strategic objectives in the IT strategy in the Ministry of Interior in 2012.

However, considering the development concepts, certain areas of concern emerge. The root of the problems is that the eWTOS tries to reflect paper-based workflow to the greatest possible extent.

Undoubtedly it has several benefits. It is an exact process having been improved over the years, known in details, the replication of which is feasible. The users are familiar with the complete process, so their training is easier compared to the introduction of a brand new system.

Besides, some disadvantages can also be seen. First is that the above mentioned paper-based process can not be replicated with100 % accuracy. The other issue is that the electronic document handling does not have as clear, widespread rules as the paper-based one. In addition, in case of electronic based document handling, such problems emerge that do not occur concerning paper based document handling, for example the missing of classified information caused by crash of terminal which can violate the principle of availability. [4]

Besides the above mentioned problems, it can be stated, that these are not the peculiarities of eWTOS, but they might occur in any electronic document handling systems. What has been said above it is clear that eWTOS is progressive not only in its solutions, but it also raises issues that might arise at other organizations in several years' time.

The future of eWTOS will probably be similar to that of other, greatly innovative ideas. After the launching of the system, it will change, will be refined according to the users' experience, while lacking or not completely existing legal regulations will be made, formed and the existing ones will also be modified based on experience.

## References

[1] Kovács László (szerk.): Számítógép-hálózati hadviselés: Veszélyek és a védelem lehetséges megoldásai Magyarországon. Tanulmány. Budapest, 2010 Zrínyi Miklós Nemzetvédelmi Egyetem p. 56.

[2] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról http://www.complex.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV – (2013.03.21.)

[3] A Kormány 2142/2007. (VII. 27.) Korm. határozata az Új Magyarország Fejlesztési Terv Környezet és Energia Operatív Programja, Elektronikus Közigazgatás Operatív Programja, az Államreform Operatív Programja, Társadalmi Megújulás Operatív Programja, a Társadalmi Infrastruktúra Operatív Programja, valamint a Regionális Operatív Programok 2007-2008. évekre vonatkozó Akcióterveinek jóváhagyásáról - Határozatok Tára 36. szám 2007. július 27. p. 263 - 277 http://www.kozlonyok.hu/kozlonyok/Kozlonyok/10/PDF/2007/36.pdf – (2013.03.21.)

[4] 2009. évi CLV. törvény a minősített adat védelméről http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0900155.TV – (2013.03.21.)

[5] 12/2012. (III. 22.) BM utasítás a Belügyminisztérium Informatikai Stratégiájáról. Hivatalos Értesítő, A Magyar Közlöny melléklete 13. szám 2012. március 22. p. 1626 - 1643 http://www.kozlonyok.hu/kozlonyok/Kozlonyok/12/PDF/2012/13.pdf – (2013.03.21.)

## Figures

[6] Figure 1. The Procedure of Written Tasking Orders
Source: http://www.nbsz.gov.hu/main.php?l=hu&p=1&a=7 – (2013.03.16.)

[7] Figure 2. The Principle of eWTOS
Source: edited by the author

[8] Figure 3. The Structure of Online Terminal
Source: edited by the author

[9] Figure 4. Workflow of Paper-based Process
Source: edited by the author

[10] Figure 5. Workflow of Electronic-based Process
Source: edited by the author