HADMÉRNÖK

VIII. Évfolyam 4. szám - 2013. december

Kovács Zoltán
zkovacs@nbsz.gov.hu

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

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. 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. With reference to this it analyses the relevant security issues, the success of those issues and the classification for the critical information infrastructure.

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. 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. Ennek kapcsán áttekinti a releváns biztonsági kérdéseket, azok érvényesülését, valamint a kritikus (létfontosságú) információs infrastruktúrává történő besorolás kérdéskörét.

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.

Review:

The first part of these series describes the tasks of the eWTOS. In order to comprehend that the article reviews the tasks and the activities of the Special Service for National Security and the process of the written tasking orders obtained from the tasking organisations. After that in the framework of a historical overview it reviews the events determining the current structure and operation of eWTOS in addition to the above mentioned issues. After clarifying the fundamentals it describes the structure and the principles of the operation of eWTOS and the similarities and the differences between the paper-based and electronic processes. Finally the incorporation of the eWTOS invented in 2005 into the IT strategy of the Ministry of Interior issued in 2012 is examined. In terms of this it establishes that the system utilizes such forward

solutions and performs such functions today which were only formulated as strategic purposes of the Ministry of Interior in 2012.

THE EWTOS AS CLOUD

The Electronic Written Tasking Order System can be regarded as a cloud computing system in terms of the Tasking Organizations requesting services from the Special Service for National Security. In order to verify this statement and classify it accurately the features and the classification of clouds should be reviewed. [2] For this the definition accepted as a quasi-standard, formulated by the Information Technology Laboratory of the NIST (National Institute of Standards and Technology) provides assistance. [3] (It should be added that according to the NIST this is a dynamically developing technology which indicates that the definitions will develop, change and refine in time.)

First of all, we must define which features are necessary to determine that a service is regarded as cloud computing. According to the definition of NIST:

- *„On-demand self-service:* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- *Broad network access:* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- *Resource pooling:* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- *Rapid elasticity:* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- *Measured Service:* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service." [4]

According to the experts of NIST these are the features which characterize the clouds applied for a given system irrespective of the service and deployment models (described later). In my opinion the existence and prevailing of these features depend on the service and deployment model the system is operated by. (This is why the compliance testing of eWTOS should be accomplished after the description of the above mentioned models.) In order to categorize the clouds and classify a system operated by this principle, if it is possible, and to do this in case of eWTOS, the knowledge of the previously mentioned two model groups with their advantages and disadvantages is necessary.

Service Models:

- Cloud Software as a Service (SaaS): *"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."* [4]

  Advantages: can be implemented quickly, employed immediately, the devices utilized by the users are wide range, it does not require great investment, the IT operation and maintenance, which is the highest costs, can be reduced significantly, the software applied is always up to date, the basic, general security functions are provided by the provider (e.g. antivirus software), the change of application can be performed quickly with low cost.

  Disadvantages: no customization or unique request service, minimal configuration potential is available, the capability of applications is given, the development and implementation of new functions are fully dependent on the provider, and its implementation requires a lot of trainings.

- Cloud Platform as a Service (PaaS): *"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations."* [4]

  Advantages: unique, even self-made software can be used, thus its implementation is quick and easy, the heterogeneous software environment is homogenized to a certain extent. The costs expended on IT investments can be reduced significantly, because systems calibrated for short-time peak loads do not have to be purchased and maintained, most of the devices used by the user can be utilized in the future too.

  Disadvantages: to update the applications installed by the user is still the responsibility of the user, the installable applications are limited by the hardware and software components supplied by the provider, therefore in case of careful choices, only a compromise solution can be achieved. Changes occurring by the provider can induce unplanned developments. It also requires a higher level IT background support by the user, so the costs expended on IT maintenance, including wages, cannot be reduced so effectively as in the case of SaaS. Even if it is possible or economical, the applications provided by the user should be recoding to utilize the advantages of PaaS indeed.

- Cloud Infrastructure as a Service (IaaS): *"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)."* [4]

Advantages: the entire, customary software environment can be transplanted, thus it can be used with the old devices, without training, easily implementable, the control of all software can be provided (except the one ensuring the visualization, but it may be the least crucial), and the implementation of a new software component, function depends only on the user.

Disadvantages: the formation, operation, maintenance and updating of the complete software environment are the user's responsibilities. On the user side almost the same information organization has to be maintained as previously, the old, obsolete, heterogeneous software environment might be conserved. From the three models this model contributes to reducing the IT costs least. [5]

Figure 1 shows the functions belonging to the responsibilities of the user and the provider in different models.

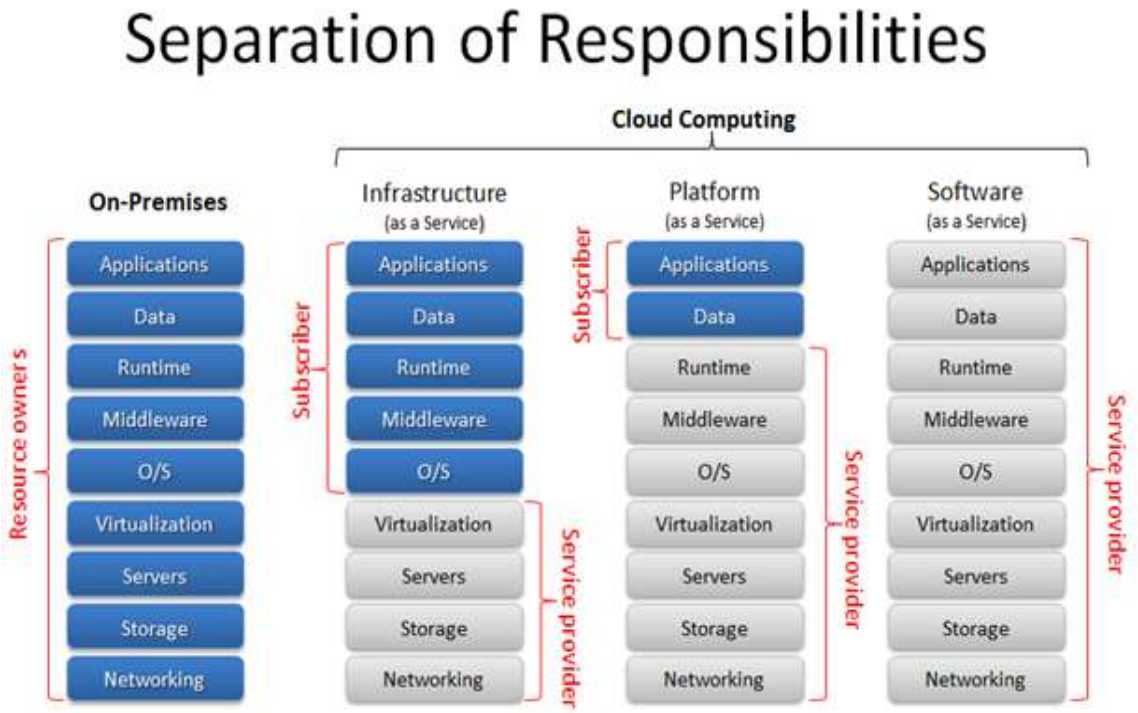

Figure 1. Separation of Responsibilities
Source: http://blogs.cisco.com/wp-content/uploads/Seperation-of-Responsibility-in-Cloud.png (2011.10.29.)

It has been attempted to complement the service models in many ways (as previously mentioned, the experts of NIST also expect a similar development process). Such concepts emerged like "*Desktop as a Service*" (DaaS) [6] (which means the virtualization of desktop systems for thin clients) and "*Process as a Service*" (PRaaS) [7] (according to which the whole process is a complete solution running in a cloud and the user does not require any intervention from the IT professionals). Even though the above mentioned three models are completely accepted by everyone – including the industrial parties as well – and use them as quasi-standards, the latter (also the ones not mentioned) are not known or not accepted and their reason for existence is questioned. [8]

Figure 2 shows who are the ones interested in and can see the advantages of the service models.

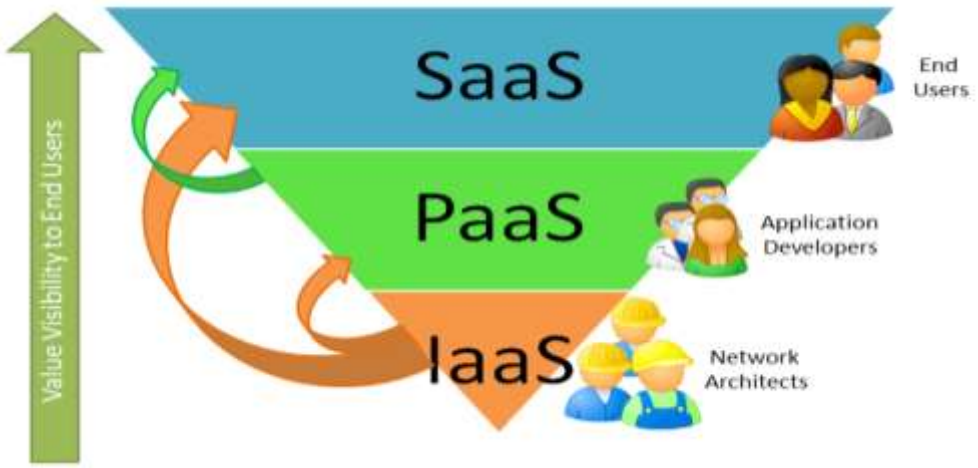

Figure 2. Value Visibility to End Users
Source: http://www.saasblogs.com/saas/demystifying-the-cloud-where-do-saas-paas-andother-acronyms-fit-in/, (2011.10.29.)

Deployment Models:

- Private cloud:

  „The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise." [4]

  Advantages: the complete system is under control, it is where the security can be ensured the most, the given systems and system elements can be utilized.

  Disadvantages: limited resources, it has to be planned for peak load, less scalable, it is where the reduction of IT costs can be managed least.

- Community cloud: *"The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise."* [4]

  Advantages: due to the common interests it can be scaled well for the given tasks, significant costs can be saved since the IT costs allocated to it can be shared, the security can be ensured, and it can be compliant for the criteria of the common interests.

  Disadvantages: besides the common interests there can be unique requirements, which can only be fulfilled by compromises or cannot be fulfilled at all, limited scalability, (in case of common interests the peak loads can appear at the same time, which can be critical or the advantage of lower costs can be lost), in certain cases the applied software, or applications should be changed.

– Public cloud: *„The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services."* [4]

  Advantages: total user mobility is ensured, good scalability, it is the most economical, only the real consumption is paid, almost maintenance-free for the user, it is where the smallest IT team is required on the user side.

  Disadvantages: problems might arise with availability, data restore, business continuity, the physical location of the infrastructure is not known, the security can be ensured the least here.

– Hybrid cloud: *„The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds*" [4] when the resources in the private cloud run out and complemented by typically public cloud [9]).

  Advantages: basically a controlled system, constructed for unique requirements, capacities necessary for load higher than the average needed to be purchased in the extent and period of unique demand, costs can be saved as no IT systems for peak load are required.

  Disadvantages: during linking the availability, data restoring and security are not ensured in a homogeneous way. The physical location, the composition, the security, etc., of the external resources are not known or limited information is available. [10]

A kind of matrix can be formed from the service and deployment models. If it is the user's decision whether some business IT services are "outsourced" to a cloud then they have to find where to place their (existing or planned) system in this matrix and they can choose the appropriate products from the fields of the matrix. Such product positioning is shown in Figure 3 on the products of Microsoft.

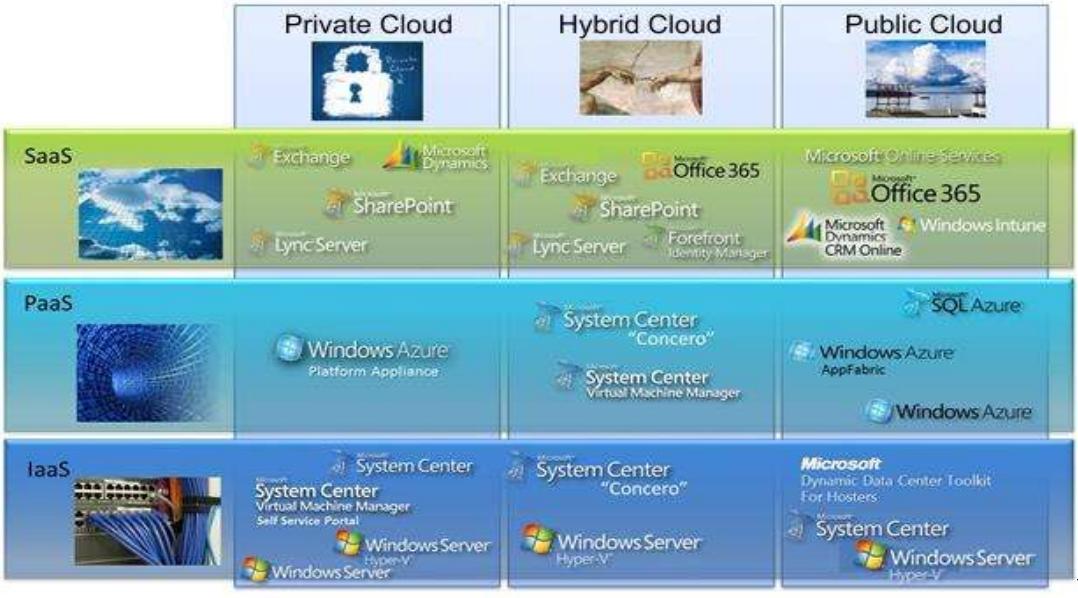

Figure 3. Product Positioning in the Matrix of Service Models and Deployment Models
Source: http://lepenyet.wordpress.com/2011/06/29/a-szmtsi-felhok-hatsa-az-itversenyhelyzetekre/, (2011.10.28.)

Figure 3 has importance from the viewpoint of eWTOS as it illustrates both the matrix formed from the service and deployment models and the fact that in different cells different software solutions are required.

The definition of NIST attempts to describe the essential characteristics of cloud computing systems in general (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service), thus it might result that features applying to a given service or deployment model do not or limitedly apply to the others. The types of the service and deployment models of the cloud computing systems are described in the broadest sense, but every existing system is different, therefore during the classification the main features should be examined.

About the eWTOS from the viewpoint of the tasking organizations as users we can claim that:

- It works as a Cloud Software as a Service (SaaS) because the services the user is supplied with are provided by the applications running in the cloud infrastructure.
- It works as a Community Cloud because the cloud infrastructure is shared by many organizations (tasking organizations, authorizing organizations and the SSNS), so it supports the common interests of the given communities (e.g. common goal, security requirements, prescriptions, compliances). The infrastructure is managed by the SSNS, the main physical elements of the system are not located at the sites of the users (tasking organizations).

The classification of the eWTOS is not difficult, but the examination of the features typical of cloud systems (according to the definition of NIST) is necessary in order to declare it is a cloud.

It can be said about the eWTOS that its services are available through networks via standard mechanisms with heterogeneous devices. The appearing requirements (e.g. operation system, minimal hardware configuration) are usually not stronger restrictive factors than other requirements appearing connected to other cloud computing systems working as a *Software as a Service*. Stronger requirements were formulated only to achieve higher level security (e.g. observing regulations of Act No. CLV of 2009 on the protection of classified information). The users (tasking organizations) do not know, or cannot control the location of the provided resources, but the capacity of eWTOS do not seem limited to them. These can mostly, but not completely cover the definitions of cloud computing by NIST. The question is whether eWTOS can be declared a cloud computing system in terms of the tasking organizations.

In this case, the fulfilment of the five examined essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service) are accomplished as in any other cloud computing systems working as a *Software as a Service*. The definitions by NIST are less typical for this kind of cloud computing systems, for instance an email service (e.g. gmail), or an online storage service (e.g. Dropbox). These features are very similar regarding both eWTOS and the above mentioned systems, so if the fulfilment of the essential features are accepted (or disregarded) and they are called cloud computing systems then it is what should be done in case of eWTOS as well.

CONCLUSIONS

This article demonstrates that eWTOS is a cloud computing system in terms of the tasking organizations, and classifies into the proper category. This is very important, because recently only few cloud systems are used by national security and law enforcement agencies. This is the reason why the experience of eWTOS should be analysed carefully.

The security elements of the IT systems are essential for the national security and the law enforcement agencies. Accordingly, it is worth examining the planned and implemented

security elements of eWTOS, and then evaluating repeatedly when the experience of using and operating is collected. This can help the developers of similar systems to develop secure cloud systems for agencies mentioned above, and users to identify the important questions and problems, which must be focused on.

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] Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél – Hadmérnök VI. Évfolyam 4. szám - 2011. december

[3] P. Mell, T. Grance: The NIST Definition of Cloud Computing Version 15, 10-7-09, National Institute of Standards and Technology, Information Technology Laboratory http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf (2011.10.21.)

[4] Lepenye Tamás: Számítási felhő – egyszerűen (2011. június 15.) http://lepenyet.wordpress.com/2011/06/15/szmtsi-felho-egyszeruen/ (2011.10.21.)

[5] Lepenye Tamás: Számítási felhő – egyszerűen (2. rész) (2011. június 16.) http://lepenyet.wordpress.com/2011/06/16/szmtsi-felho-egyszeruen-2-rsz/ (2011.10.21.)

[6] Enrico DePaolis: Types of Cloud Computing (2009. július 25.) http://cloudcomputing.sys-con.com/node/1048046 (2011.10.09.)

[7] Louis Naugès: PRaaS, Process as a Service (2009. augusztus 30.) http://nauges.typepad.com/my_weblog/2009/08/praas-process-as-a-service.html (2011.10.22.)

[8] Dan Kusnetzky: Fourth type of cloud computing (2009. október 5.) http://www.zdnet.com/blog/virtualization/fourth-type-of-cloud-computing/1346 (2011. 10. 09.)

[9] Bharath Chandrasekhar: What is Cloudbursting? (2011. március 15.) http://cloudsecurity.trendmicro.com/what-is-cloudbursting/ (2011.10.22.)

[10] Lepenye Tamás: Számítási felhő – egyszerűen (3. rész) (2011. június 17.) http://lepenyet.wordpress.com/2011/06/17/szmtsi-felho-egyszeruen-3-rsz/ (2011.10.21.)

Figures

- Figure 1. Separation of Responsibilities
  Source: http://blogs.cisco.com/wp-content/uploads/Seperation-of-Responsibility-in-Cloud.png (2011.10.29.)
- Figure 2. Value Visibility to End Users
  Source: http://www.saasblogs.com/saas/demystifying-the-cloud-where-do-saas-paas-and-other-acronyms-fit-in/ (2011.10.29.)
- Figure 3. Product Positioning in the Matrix of Service Models and Deployment Models
  Source: http://lepenyet.wordpress.com/2011/06/29/a-szmtsi-felhok-hatsa-az-it-versenyhelyzetekre/ (2011.10.28.)