2017/3

American Journal of Research, Education and Development

RED

ARS SCIENTIAE
DEV L'ART
SCIENTIA ARTIS

ISSN 2471-9986

American Journal of Research, Education and Development

IMPRESSUM

American Journal of Research, Education and Development
ISSN: 2471-9986

Publisher: DEVLART LLC
250 Camelback Ridge Ave. Henderson, NV 89012
red@devlart.hu

Editorial Board:

Editor in Chief:
Prof. dr. Gyula Kóródi MD. PhD
National University of Public Service

Managing Editor:
Dr. János Rikk
National University of Public Service
rikk@devlart.hu

Associate Editors:
Dr. Zsolt Haig
National University of Public Service
Dr. László Mészáros
University of Kaposvár
Dr. Marko S. Markov
Research International
Dr. Zsolt Radák
University of Physical Education
Dr. Imre Négyesi
National University of Public Service
Prof. Dr. Klára Kecskeméthy
National University of Public Service

CONTENT

Design a small business computer network (case study)

Péter Török, Dr. Imre Négyesi

National University of Public Service, Hungary

Abstract

The expansion of the computer network is one of the most significant way of innovation. The need for the expansion of computer networks is required by the display of newer technologies, new networking methods and tools. The need for expansion is further increased by the users' rising demand for local and web networks. The users apply more and more network services on their computers; the use of mobile tools for the continuous reach of remote networks is getting more and more widespread. These needs can only be satisfied by the computer networks by giving ground to continuous development.

Keywords: SOHO, network, computer environment

Introduction

Entertain BT was approached via e-mail by the CEO of Nagy-ker Nagykereskedelmi Kft to request a preliminary survey about designing a computer network for the company's new site.

Before we start the preliminary survey, let's clarify some elements we will use during our work.

The expansion of the computer network is one of the most significant way of innovation. The need for the expansion of computer networks is required by the display of newer technologies, new networking methods and tools. The need for expansion is further increased by the users' rising demand for local and web networks. The users apply more and more network services on their computers; the use of mobile tools for the continuous reach of remote networks is getting more and more widespread. These needs can only be satisfied by the computer networks by giving ground to continuous development.

The development can be materialized by taking the following aspects into account:

- the realization of more physically extensive networks
- bandwidth expansion
- applying new methods and tools
- development of data transmission methods
- formation of a scalable network
- formation of fault-tolerant systems.

For unified interpretation let's review some of the elements.

Bandwidth (transmission speed): The number of bits passing through the data transmission channel (wired or wireless network) per second. (Unit: bit/sec [bps], For the expansion of bandwidth it is often sufficient to develop a new data transmission method on the already existing wired or wireless medium, the latter often does not require change.)

Delay: The delay is the amount of time required for the transmission of packets trough network connection. Factors influencing delay may include:

- endpoints (computer, pda, mobile phone, network printer), which code/decode their network messages in the form of a digital sign for a network medium
- network medium (wired and wireless)
- network intermediary tools (switches, routers).

For the measurement of delay, under Windows for example, the tracert command is used, which shows the passing of network packages trough routers and their delay.

Response time: The period of time a network system requires for responding to the need demanded by the sender. (Typical measurement tool is the PING command, which shows the response time of the package.)

Scalability: One of the cornerstones of the expansion of networks is to design the already existing network in a way, so it's capable of carrying out future extensions. The scalability is feasible trough the extension of a few network tools (e.g. switch), but a WAN-connection (backbone network) tool (router) may be needed to increase the performance..

Fault tolerance: Before discussing the fault tolerance as a new term, let's say a few words of the concept of availability. The availability of network systems usually means a number given in percentage which outlines the constant operability of the network in every moment of the year. The internet provider must provide this number, because it's the customers contractual right to know that what amount of network failure they can allow. In case of business customers even a moment of network failure can cause serious problems and losses. This is why we must create a fault tolerance system, so redundant connections help the fault tolerance and continuous availability of the system.

Beyond the aforesaid details the computers can be tabulated by the size of computer network, operation, transmission method, and many other aspects,

- extent of the network (PAN, LAN, MAN, WAN),
- network topologies (bus, ring, star, extended star, tree, web),
- technology type of data transmission (broadcasting networks, point-point networks),
- network technology implementing data transmission (Ethernet, TokenRing, FDDI).

If we want to illustrate the hierarchy of a large-scale network, we can divide it into three parts

1. The elements of the end systems are devices suitable for running network services (applications), which can be found on the edge of the network. (Such as the computer, server, network printer, PDA, IP-phone, mobile phone etc.).
2. The access networks are appliances (routers) connecting the end system to the network's higher level line, possibly appliances (routers) connected to its ridge line. (These networks may be home, business, or mobile /wireless/ networks as well.).
3. The network core connects the package switches of the end systems with the backbone network of the internet. The core of the network consists of the internet service providers (ISP), regional access providers, and the backbone network. The internet service provider has a point of presence (POP). The POP is the connection point, trough which the business clients can log in to the network. The regional access provider connects POPs belonging to multiple internet service providers, and connects them to a larger scale network.

Lastly the backbone network consists of multiple high speed, high capacity private networks (national providers). These networks overlap, so they can provide bigger capacity, traffic, better load balancing, and reliability. The appliances forming the core of the network can switch the data trough data networks in two ways: circuit switching and packet switching.

There are different methods for switching stations.

Circuit switching: The circuit switched networks occupy the communication channels between the end systems for the whole duration of the session, and the connection lasts until it is interrupted. Phases of circuit switching: building the connection, maintaining and using the connection, and lastly, dismantling the connection. (Analog telephone technology also operates on this principle. It is not economical; today it is occurring in smaller and smaller numbers. Very expensive, slow and isn't capable of reliable data transmission.).

Packet switching: In today's modern computer networks the source breaks the message up to smaller packets. Packets received this way pass through a communicational channel and packet switches between the source and the destination. Before reaching their destination the packets travel on variable routes, and only occupy the given communicational channel until they pass the given packet switch. It is also possible, that the packets have to wait at some of the packet switches because of the accumulated amount of data traffic. (Packet switching is the most common switching method of these days.)

Based on the facts stated above we can say that the network is a very complicated system in terms of structure, which consists of many applications, different kind of end systems and switching methods. To understand the whole system, we must divide it into multiple layers. The layered architecture makes it possible for us to concentrate on a given module of a complicated system. The layered network model is also required for the communication of the appliances made by the network manufacturers between each other, using an appropriate protocol language. The under mentioned models provide an individual service for each layer, which is provided for the layer above it. In other words every layer provides its service by carrying out given tasks inside the layer, and also using the services of the layer below. This is the service model. Inside a given layer the end points apply rules, and they can send messages for each other with this. This is called protocol. The protocol of the different layers are called protocol stack.

After all these, let's take a look at what specific steps do we have to follow while designing a network.

Network design is the first (and fundamental) step of building a network. A network that was not designed properly won't be able to complete its tasks, and the costs of later changes and repairs may even exceed the cost of building it.

The main aspects of designing today's networks (keeping in mind to try to create the most useful network for working using the tools available):

- creating a flexible, reconfigurable network;
- creating a network that satisfies the needs of the future, with possibilities of expansion;
- taking data protection aspects into account;
- providing safety from noises and environmental impacts of foreign origin;
- to meet the requirements of both national and international regulations and standards;
- to be able to serve an appropriate number of end points.

The process of designing can happen in multiple steps:

- designing IT systems (servers, workstations),
- making a network system design,
- making plans of structured local area networks (LAN)
- making plans of structured wide area networks (WAN).

In parallel with the aforesaid the next task is to make a network system design, in which we specify the requirements and parameters of the system to be built, and designing the actual structured network takes place only after this. The cabling and the path design, the installation of appliances and tools according to the standard, and transfer – receipt proceedings must be developed. The plans of structured wide area networks include the description required services, and the selection of the most suitable router. It is also an important rule of design that the segmentation and the development of the VLANs must be done in a way that the workstations belong to the logical network which contains the servers most frequently used by it. This way the load of the ridge direction can be reduced. These are the possible methods of reducing the load:

- Relocation of resources in order to keep the traffic inside the work group.

- Logical relocation of users in a way that the work group can reach the given user more directly.
- Expansion of servers in a way that instead of the ridge they are locally available.

The company

At the request of Entertain Bt, the following summary was delivered by the Chief Executive of Nagy-ker Kft.

"Our company was founded in 1994 under the name Nagy és társa élelmiszeripari Kft. In the beginning, our main field of activity was the production of seasonings and spice mixtures, and we are dealing with the distribution of raw materials and accessories for catering and public catering. Our market has been rapidly developed nationwide, so we are now among the first in Hungary with similar product manufacturers and traders. We have grown our first site, so in 1999 we opened a new site for our increased turnover. In the new place, we built a Cash and Carry store, where we expanded our range of warehouses, catering to confectioners and bakeries.

In 2000, we opened up to a new market segment, we added our palette with "bio" gastronomic articles, expanded our range of products with foodstuffs used in catering and bakery industry, creating a significant turnover, and today our annual turnover is over HUF billions. Our primary trading areas are Budapest, Pest county, in these areas we have developed our hiking trails mainly along the M1 and M7 motorways.

In our C + C store we sell to our crawler customers in a self-service way, but we make a significant part of our turnover with delivery. Our logistics background provides our customers with a daily service that we operate under our HACCP quality assurance system.

Our partners can place their orders by phone, fax or e-mail (vevoszolgalat@nagy-ker.hu) or on our web site (www.nagy-ker.hu) at our customer service.

The company currently employs 44 people in three main organizational units. There are 12 employees in the economic sector and 4 managers. There are 6 people in the store, customer service, billing and cashier, and 8 are salespersons. In the warehouse are 8 people and 6 drivers. "

The project

The size of the network was surveyed during site navigation. Proper installation of network distributors does not require the installation of new signal amplifiers. Workplaces in the three main areas of activity are physically separate. A total of 80 network endpoints will be created for the computer network in 18 rooms.

During a long discussion with the management, the services and the required software environment were clarified.

The company has its own domain name, the related webpage is placed on an external server. The maintenance of the website is carried out by an external company. This does not need to be supported by the network to be established.

The domain mail server, however, is deployed at the company's premises, stores incoming mails on its own, and performs mail forwarding and forwarding independently.

The Internet connection of the site, Internet access for workstations should be regulated locally, and the structure to be developed needs to be supported.

Attacks from the Internet must be protected in a number of (overlapping, complementary) ways.

On a local area network, documents are stored in the directory structure to be created on the server, with access to more access levels at different levels.

Virus protection for servers and workstations, including virus protection for e-mail traffic, must be secured in a prominent way.

In addition to the wired network, wireless (Wifi) access should also be provided. Separate for employees, full network functionality and specially for buyers, guests, visitors only for Internet access.

Client-to-business retailers should be provided with remote access to the local area network. This is only in a reliable, secure way. Among the solutions to be considered, the design of VPN won the leadership's liking.

The company uses customized enterprise management software, which includes inventory inventory records, booking orders, compilation of delivery notes for deliveries and billing. It has a database connection to the accounting software. The program is running on a web interface, so a web server must be installed on the server.

Data and documents stored on the server should be backed up regularly, with the appropriate backup strategy and backup and archiving program required.

It is necessary to ensure the continuous operation of the server, requiring the provision of a suitable, manageable uninterruptible power supply.

The right of access to, and access to, the employees of different fields of activity must be well separated when network is established so that the integrity of the system remains.

Print under centralized control with 10 independent printers.

Designing the hardware environment

With the necessary data you could start planning.

First, summarize the tasks to be performed by the server:

- a file server for storing local users' documents
- printer management to manage 10 network printers
- rescue-archiving solution for documents stored on the server and for correspondence
- a web server to support enterprise software
- mail server, imap and http connectivity
- a packet filtering firewall for the network to protect external attacks
- a central antivirus system with real-time web, mail and file protection
- network address translation to secure Internet access to workstations
- handling VPN connections for remote work

Taking into account the number of users, workstations, and printers, resource requirements for tasks can be met by running a server. This simplifies network administration, no central user management system is required.

After defining the hardware requirements for the server, the number and location of the network devices was determined.

The obvious solution of the separate network structure requested by the customer is breakdown into VLANs. Thus, at the boundaries of the subnets, traffic can be limited by a separate rule system if appropriate Layer3 manageable network devices are used.

The server and network devices are placed in separate VLANs to isolate and protect network devices. The scope of activities is put into separate VLANs, so traffic between them can be restricted or restricted and can be controlled separately by the server.

Separated access for employees and external users was a consideration when designing the wireless network. This can be done by building a dual system or using MultiSSD support tools. In the first case, the network is expensive, the second is the price of access points. Based on the sketches made during the scenes, the number of devices required can be determined. There are 2 in the office, 3 in the store, 1 in the warehouse are needed for proper coverage. Therefore, using the MultiSSD support tools, it is worth solving the dual Wifi network.

Documentation

Based on the needs and the considerations arising from the discussion and planning, the following design documentation was compiled:

This document contains a system design for the IT infrastructure and services of the Nagy-ker Nagykereskedelmi Kft. (Named Nagy-ker) (name conventions, discrete system, network settings, IP domains, IP addresses, passwords, operating system and application versions, management system, firewall policy system, WIFI system)

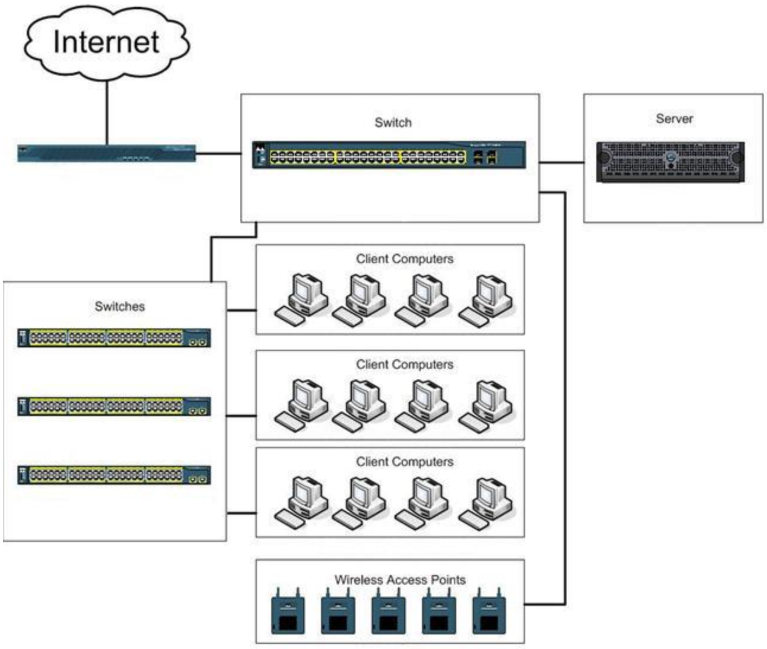

Fig 1. General graph of the network of the Nagy-ker network

User environment on workstations

Hardware

Workstations purchased by Nagy-ker have a unified hardware environment, which greatly facilitates system administration.

Optional Windows 7, Windows 8, Debian Linux Software Environment

Creating a unified software environment in the operating system and the office software environment. For different uses, it is necessary to create multiple operating systems on client machines

Efforts should be made to use as little resources as possible for administration. Improved patches can be distributed centrally in the unified environment. Software failures do not require repair, but the preinstalled software environment can be deployed automated to the workstations to minimize the duration of repairs.

Since client computers can not be dedicated to users, and there are likely to be attempts to modify configuration settings or install software, it is recommended to create the most stringent user access system.

Centrally managed antivirus system

Critical in the antivirus environment is the automation, which can be used to quickly fix the updates, to change the configuration settings centrally, to make the user's intervention impossible. You must also ensure proper logging, which helps you to track virus infections and other events on your clients (such as successful updates). Since workstations can be used for removable media (such as a pendrive), there is a need for enhanced security at the workstations (real-time monitoring of all files that can not be turned off).

Not only need workstation level checks, but also need to filter on a server site (mail server antivirus, Internet traffic monitoring)

Windows network

Workgroup

A working group will be set up for easier administration. The NetBIOS for the Workgroup is NAGY-KER.

Computer name conventions and settings

Basic considerations

In order to simplify system operation, it is important to design a name convention when designing a system that will prevent the computer from being compromised. For servers, you have to choose names that you will not have to change later on. For workstations, frequent change of name may result in administrative overhead work, so it is advisable to create a structure that avoids changing names as much as possible, but the location and user of client computers can be solved using the inventory database.

Kiszolgálók elnevezése	function in brief	OS
name of the server		
srvlin01	DHCP, DNS, file, mail, print, web	Debian Linux 7.3 64 bit

Conventions for User Names and Groups

Basic considerations

Because the Great Circle network can be separated into distinct user roles, it is therefore necessary to define uniform rules and ensure that user names are unique.

Employee's User Accounts

Currently, usernames consist of the first character of the first name and the nickname of the surname. If matching, the first 2 letters from the name, 3 letters for further matches, etc. should be used. For full matches, numbers are allowed. For example: István Szabó: iszabo, isposo, ist'lo, istvanszabo2 etc.

Name Groups

In all network infrastructures that aim at establishing eligibility levels, it is necessary to provide groups to facilitate the administration and registration.

Naming service accounts

Creation of special users for the operation of the system on which the services required for each system are run on behalf and with the rights - if this can not be avoided.

The password must be handled in accordance with the appropriate security requirements.

Special accounts should not be used for interactive login, for each application it must be resolved that it can be administered by operating personnel using the appropriate security groups.

Network settings

When designing a well-functioning network infrastructure, it is essential to develop the right VLANs, primarily based on security and performance considerations.

According to the current concept, Nagy-ker uses the commonly used private IP addresses with the correct translation. The range used is 172.16.0.0

VLAN ID	VLAN name	VLAN Network ID	Subnet Mask	Default Gateway
2	Default	172.16.2.0	255.255.255.0	172.16.2.254
10	Servers	172.16.10.0	255.255.255.0	172.16.10.254
11	Iroda	172.16.11.0	255.255.255.0	172.16.11.254
12	Raktar	172.16.12.0	255.255.255.0	172.16.12.254
13	Uzlet	172.16.13.0	255.255.255.0	172.16.13.254
60	WIFI_Internal	172.16.60.0.	255.255.255.0	172.16.60.254
61	WIFI_External	172.16.61.0	255.255.255.0	172.16.61.254

Table 1. The structure of the IP address of the Nagy-ker network

Network services

DHCP

The main benefits of the service:

The DHCP service allocates network addresses, making it significantly easier to keep records and avoid collisions. You can also set client settings for networking, so any configuration settings can easily be distributed.

The DHCP service was installed on the srvlin01 server.

other parameters

IP address:

Subnet mask 255.255.255.0

Getaway (172.16.x.254)

DNS server (172.16.10.1)

DNS domain name: nagy-ker.local

Set up DNS registration for DHCP-assigned addresses.

Address Rental Time: 5 Days

DNS service

As one of the most important elements of network communication is the DNS service, it is necessary to pay close attention to its design. Important is the automatic update, reverse zone and replication.

The srvlin01 server performs these services with the following settings:

There is a forward zone, zone name: high-level zone

Configure the Forwarder to the Server (ISP later assigned NS)

When creating reverse zones, all subnets (zones 172.16.x.0) have to be added, their settings are the same as the forward zones.

File server, security settings

Home folder

Each user account has a home directory with appropriate security settings, which is automatically connected. You will have to create the WORK, EXPORT, IMPORT directories automatically.

Joint folders

More common drives must be created in the structure specified by the Customer. It's a good idea to create an ACL if someone does not have the right to a directory, then you can not just log in, but do not see it in an administrator.

Recommended quotas:

Warehouse, business workers for home directories: 100 Mbyte

Employers working in home directories: 500 Mbyte

For shared libraries: 1 GByte, which of course depends on the number of libraries.

Remote access:

Because shopkeepers may be justified in accessing the file server remotely, it is necessary to create the ability to access files (for writing and reading) over the Internet. It is recommended that you use VPN to access local network resources over the Internet.

Security settings

Server security configuration:

When installing all of the server services, make sure that the same settings and components are installed for ease of administration (obviously, exceptions are the target functions, such as DNS, DHCP, etc.).

During installation, you must disable any component that the installer offers.

Rename local administrator (from Group Policy, set a complex password.

Logging events that are important for traceability (login, unsuccessful operations, etc.) should be carefully archived.

Client security configuration:

Clients have user rights on workstations. The Windows 7 and Windows 8 operating system level defaults are appropriate for using such a limited account because no configuration options can be changed and access to system files is prohibited.

Password policy:

Password expires in every 90 days

Alert 14 days in advance

Locks the account immediately after the expiration

The password must be different from the previous one in at least 5 characters

Password length minimum 7 characters, complex (lower case, upper case, numbers)

When creating a user, the default password is the birth date (8 characters).

For operator personnel, it is particularly important to enforce these rules because the most critical users are here.

Management and antivir

LanDesk Management + Antivirus Suite 8.8 is installed in the Nagy-ker network.

Features to be introduced:

Hardware Inventory,

Software Inventory,

OS Deplyment,

Software Distribution,

Remote Control,

Antivirus console.

To use this system, you do not need to distribute functions between other servers, you just need to install it on a featured client. The system can be controlled from a console, managed by software deployment, operating system distribution, antivirus control.

Workstations can be remotely deployed by agents, but since it is installed at the same time with Landesk imaging technology, it is more convenient to integrate the operating system image.

WIFI

Since Wifi devices are capable of MultiSSID, it is advisable to configure a multi-level wifi system (to enable or disable internal resources).

VLAN 60

SSID: NAGYKER_private

Authentication: wpa, with a predetermined key

Internal resources are available as internal clients

IP Range: 172.16.60.0/24

VLAN 61

SSID: NAGYKER_public

Authentication: wpa, with a predetermined key

Internal resources for customers are not available, only DNS name resolution, http and https outwards. Further, there is a need to limit bandwidth.

IP Range: 172.16.61.0/24

Firewall

As the system is built into a fundamentally closed organization, it is reasonable to limit the Internet traffic radically. Of course, not all ports should be banned outward because it would make work harder.

Currently, the public IP domain is not yet known because it does not have an ISP contract. As you know the outer domain, you must change the rule system anyway.

Inwards: SMTP, VPN, http and https for srvlin01

Outwards: ICMP and the following TCP and UDP ports:

37, 43, 46, 53, 79, 80, 109, 110, 119, 123, 143, 389, 443, 500, 524, 554, 563, 13, 17, 21, 22, 23, 25 (srvlin01 only) 569, 636, 993, 995

Internet access

To increase security, ASA has to create a privilege user that can edit the ACL.

References

Török Péter, Rikk János: New methods to protect our network systems; AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT 2017:(1) pp. 4-16. (2017) ISSN 2471-9986

Szabó András: A felhasználók digitális lábnyomának, anonimitásának vizsgálata technikai szempontból I. Rész - személyi számítógépek, Hadmérnök XII. Évfolyam „köfop” szám – 2017. Október

Török Péter, Rikk János: BASH scripting; Henderson: DEVLART, LLC, 2017. 68 p. (ISBN 978-0-9977210-6-5)

Laura Chappell: Network analysis; 2nd edition Chappell University 2013. ISBN 1-893939-9-1

Engineering science researches and effective government (Part 1.)

Bleszity János; Földi László; Haig Zsolt; Nemeslaki András; Restás Ágoston
National University of Public Service, Hungary

Abstract:

By the Research, Development and Innovation Strategy of the National University of Public Service "State and Governance Sciences" deal with the existence, operation and key aspects of the state and governance with common application of state oriented researches of different branches of sciences. Methodology of state and governance researches can be characterized with comprehensive approach and transdisciplinarity.

The aim of the authors is to investigate the relationship between state and governance sciences and engineering sciences and present the main areas of international technical researches focusing on coherence with state and governance. Based on this the authors specify the main state and governance related domestic technical research directions concerning the operation and security of the State.

Because of the size of the material the paper is published in 2 parts. This first part covers the introduction, the description of the relationship between engineering researches and state and governance sciences and the summary of related present international engineering researches in the fields of ICT technologies, information (cyber) security and environmental security

Keywords: State and Governance Sciences, Engineering Sciences, Horizon 2020

INTRODUCTION

The impact assessment of the technical improvement's impact on the operation of the state is very important from a scientific point of view. The radical transforming effect of the internet for example swept through more and more industries from the middle of the nineties, completely reshaping their structure and operational model. The media industry, vehicle industry, retail, tourism, education, and healthcare were greatly changed in the last 25 years. The technical improvement changed the method of production, the interest ratio of the participants, the characteristics of the products and services, and the skills and knowledge required for employment. By investigating this area we can see that the operation of the informational economy and the increase of wealth have a narrow cross-section, which is the deficiency in the reflection of the operation of the state in the informational age.

The relations between technological-technical improvement and state and governance science are not free from problems at all. On the one hand, the government's and state's demand does not generate technical improvement necessarily. On the contrary: long historical periods passed without significant technical improvement reflecting on the state's demands. On the other hand, the technical improvement does not increase automatically the infrastructural power of the state either (think about the everlasting circulation of the fight between high-tech criminals and high-tech police). [1]

In the relationship of state and governance science and technical improvement it is important to mention the relation system that the governments have a great influence on the systems of scientific discoveries: significant geographical discoveries (e.g. Columbus' journey), whole branches of mathematics and game theory (operation research), or supersonic flying, are the "civilianized" results of government and military purpose developments of computers and the internet.

The research of technological and techno-economical paradigms [1] is lie on the periphery of state and governance science and public administration science, hence understanding many narratives and phenomena related to the changing role of the state and its relation to the different systems of society and the economy may be quite difficult [2].

The scope of science-technique theories[1] is one of the trans-disciplinary directions that could strengthen and make it relevant again, and can also evolve its added values in contrast of other sciences (eg. of law science, political science, or management science) [3]. The researches in these areas systematically examine the two way relations between the expansivity, depth, and nature of state power, the particular technical inventions, and the technical improvement in general [1] [4].

[1] Science Technology Studies

Based on all this the aim of the study is to examine the relation of state and governance sciences and engineering sciences, present the main directions of international researches in the areas of engineering sciences, focusing on the relationships with state and governance sciences, and to define the main directions of local researches in relation to the operation and safety of the state based on this.

1. THE RELATIONSHIP OF ENGINEERING SCIENCE RESEARCHES AND STATE AND GOVERNANCE SCIENCES

According to the Research – Development and Innovation Strategy (RDIS) of the National University of Public Service (NUPS) state sciences are dealing with the questions of the existence, operation and government of the state, which can be examined trough the combined appliance of all the researches of social sciences related to the state. [5] The method and results of state research is characterized by comprehensive approach and transdisciplinarity. The new frameworks of state and governance science are characterized by the research of the questions related to law, public administration, defense (law enforcement, national defense, disaster protection), public order and safety (national security), and other questions related to state and society. Based on this approach we can see that the state sciences mainly prevail in the area of social sciences, however, it must also be seen that to ensure the efficient, sustainable and safe operation of the state technical researches and the use of their results were always necessary. This is only intensifying in the 21st century, because significantly new technologies and challenges appear during the operation of the state. The use and exploitation of all these technologies, and the handling of the challenges cannot lack the use of up-to-date engineering scientific results. Based on all this although the engineering sciences are not a part of state sciences, however, thanks to the close relationship system of these two even the RDIS treats technical researches as a priority.

One of the important appearances of the results of university level research is education, improving its quality and constantly and gradually integrating the results into the curriculum. One of the parts of technical nature education development pointing towards a good state is referring to the development of the role of already existing curriculums in higher education, and it also focuses on the possibilities of its IT based usage outside of higher education. The previous, by the reinforcement of the technical nature – in accordance with the university’s strategy – is a mostly evolutional development, which is based on the new approach of the public service system, which is IT based (e-learning, webinary), it also prepares the opportunities of education out of the bounds of traditional higher education in both local and international scenes. Forming a suitable infrastructure and humane environment, referral and attendance of respected guest lecturers, and the improvement of the preparedness of our own lecturers, their international reinforcement is also necessary.

The education developments towards a specified direction include the evaluation and processing of the early experiences of bachelor and master courses, their adaptation and correction to the current conditions, its development, its internationalization, preparation of the opportunities of education beyond universities, overall, further developments aiming to reach the future's strategic goals. All these tasks have to be carried out in the courses where technical questions are relevant, and within the boundaries of the university, in accordance with its strategy, by the reinforcement of the technical nature.

The relationship of state and governance sciences and engineering sciences can be best observed in the usage of information and communication technologies (ICT), and the examination of their effects in the broader areas of public service. In the central and local public administration this mainly aims the to improve the efficiency of the processes, to reshape administration culture, to reduce the administrative burdens of civil and corporate clients and to introduce new services.

In this regard the research field is in close harmony with the "National ICT Strategy 2014-2020", the pillar of the so-called digital state, but it also fits into the other three directions of development mentioned in the strategy, namely into the digital infrastructure, digital competencies, and the development of digital economy. [6] From these the NUPS educational mission specifically helps the adaptation of SMEs and public administration ICTs – improving the so-called e-acceptance - by the development of digital abilities. Horizontally at this point a very tight coordination and cooperation is possible with the organizational innovation and human resource workshops of the research community.

The "Public administration and service development strategy 2014-2020" document and the Public Administration and Service Development Operational Program priorities derived from it designated two important areas in correlation with the digital state. The implementation in the broadest possible range of the interoperability of the specialized systems, the modernization of registers, and the elimination of data redundancy are priorities.

The international trends in addition require the research workshop to ground the subsequent strategies which are capable of making e-democracy, e-attendance, e-vote and an intensive civil participation possible in virtual space too.

The increasingly intensive presence of the state's operation in the virtual space elevates information security and cyber protection the most important horizontal research fields amongst ICT applications not only in Hungary, but also internationally. The "National ICT Strategy 2014-2020" fitting horizontal factors emphasizes that the maximal protection of the handled data and the critical informational infrastructures from the viewpoint of e-public administration services must be achieved; safety consciousness must be evolved; user groups must be prepared in terms of actual safety hazards and their handling methods, with special attention to the safety of the children. [6]

In parallel with this (amongst other things) the NUPS developed serious capacities in the past few years in the areas of civil public administration, home defense and policing, based on which the research community wishes to connect to other workshops by special researches: general security studies, cyber warfare, and cyber crime. It must be emphasized that information protection in addition to safety questions also includes data and information protection, in which the Faculty of Science of Public Governance and Administration and the Faculty of Military Sciences and Officer Training have high capacities and is capable of connecting the technical challenges of the virtual space with the legal regulation, security awareness and the tasks of leadership and organization in relation to the modern state administration.

In the field of environmental safety there are excellent examples of the cooperation between the different fields of public service. Trough the research of the technical questions of environmental safety certain elements appear that can also be used in several fields of state and governance sciences. The performance of public service tasks and the two way relationship system of environment safety can be observed in any field, so certain activities cause environmental impact and risks, where the research task may be to improve environmentally friendly technologies, to reduce the ecological footprint, to develop and operate environmental management systems. On the other hand, the environmental damages, environmental challenges, global environmental problems cause such a constantly changing conditionality, that affects the entire verticality of public service, and for the sake of planning and completing the tasks they require the proper handling of effects such as the reduction of environmental effects (fossil fuel, drinking water, soil, air, biodiversity), the pollution of environmental elements, global climate change, increased noise, the dangers of vibration or radiations or the problems caused by waste.

For completing the tasks of the broader interpretation of the defense sector (home defense, law enforcement, disaster recovery, and national security) – as the depository of the safe operation of the state – a wide range of technical tools and systems and technological methods are used. These technologies cover the whole spectrum of engineering sciences, starting from electronic, communication and IT systems, trough engineering to architectural and logistic systems. Military engineering is a separate special field, in which the researches related to the use of other engineering sciences for defense purposes take place. The research directions and their results materialize in the broader interpretation of defense and public administration sector and in the modern, new method- and toolkit of the application areas. Here belongs the defense industry, defense electronics, IT and communication; national defense; law enforcement; environmental security; environmental protection; protection against chemical, biological, radiological and nuclear weapons and non-proliferation; fight against terrorism; disaster recovery; protection of critical infrastructures; energy safety; and safety technology. [7]

For the development and improvement of the cooperation of organizations responsible for the defense against disasters the support of researches related to the coordinated and effective implementation of disaster recovery tasks of preparation, protection, and reparation phases is needed. The research activity primarily concentrates on law administration and technical researches related to the development and improvement of the law and institution and tool system establishing the operation of fire safety, citizen safety, and industry safety specializations. The disaster recovery researches must adhere to the research activities of universities on state and governance sciences, public security, and home security. The disaster recovery technical researches must serve the purpose of increasing the society’s abilities against disasters, reducing its vulnerability, helping it to return to its normal operating order as soon as possible, and increasing flexibility.

The classification and subdivision of disasters may differ depending on literature; however, the researchers mostly accept that considering the way of generation there are natural, and man caused disasters. Within these the classification may differ, but they mostly follow the everyday comprehensible divisions, even until total simplification; such as floods, flash floods, earthquakes, the release of radiating or dangerous substances or disasters caused by large-scale forest fires.

Considering the characteristics of disasters, we can almost always associate to significant dimensions, the delay in time of the disposal, the mandatory cooperation of different organizations taking part in the disposal (federal, civil, voluntary), or the requirement of surplus resources. These latter statements have a privileged role from the perspective of technical researches, because although the resources at hand are always scarce, this is particularly true in the time of disasters. The degree of scarceness fundamentally defines the effectiveness of the intervention and the reparation, so its reduction – with the use of new technical tools, technologies, methods and regulations – is not only an opportunity for professionals and researchers, but – in favor of reaching the goals of a good state – its also a moral obligation.

The social expectations of a good state definitely require the effective prevention of disasters, fast intervention in case of occurred events, and the fastest possible reparation, in other words greater resilience against disasters, less vulnerability and greater flexibility required for adjusting back to normal life. From the background of these the technical and methodological improvements and their related training tasks are indispensable, thus the social expectations from a good state and effective disaster recovery are inseparable. This is why it is declared in the law of Disaster recovery that the defense against disasters is a national matter. [8] [9]

The elimination of disasters is always tool and technology demanding task. However, the development level of the used tools, technologies and methods also determine the abilities of the intervening; and this latter strongly correlates with the effectiveness of elimination. It follows from the above mentioned that engineering sciences require an interdisciplinary approach from the side of disaster recovery; however, it is clear that they are also inseparably linked to state and governance sciences, and they contribute to the improvement of the qualification of a good state.

The multiplication of extreme weather phenomena caused by the global climate change, the higher level and constantly changing technical standard, the local and international commitment to protect the environment, economical and social globalization, and the increasing social sensitivity of the developing world are all suggest that the duties of the efficient disaster protection cannot be treated as a onefold act. The renewal and constant improvement of courses is indispensable for effective protection and prevention, which must be connected to higher education. In the light of these, the improvement of and education technology and course management providing an environment conducive to more effecting learning, and its increase to an international level improves the efficiency of defense against disasters.

2. MAJOR RESEARCH PRIORITIES APPEARING IN CERTAIN FIELDS OF ENGINEERING SCIENCES

The emphasized role of technical nature researches can be observed in the European Union’s Horizon 2020 (H2020) K+F program, because they are present in every pillar of the H2020, so also in the areas of excellent science, industrial leading role and social challenges.

The H2020 covers the development of the innovation chain from base research to product development. In line with this a significant part of the H2020’s work program wishes to support nearutilization innovations. The technical subject researches also have a fundamental role in the field of EU policies, such as healthcare, aging society, climate change, environment, energy, traffic, and the modernization of the public sector.

From the perspective of the relationship system of state and governance sciences and technical researches we can highlight "excellent science" and "social challenges" pillars. The excellent science supports the research of new technological opportunities in the field of emerging technologies[2], while on the field of research infrastructures dedicated sources supply the development of e-infrastructures. The aims of future's aspiring technologies are expanded with the multidisciplinary, technology-oriented, long term European researches. Amongst its highlighted areas there are cognitive ICT; quantum simulation; the science og global systems; and high performance IT.

The social challenges pillar also shows a close relationship with technical field researches, because the application of different technologies is one of the important elements of the treatment of challenges. In this field the technical technological development can be associated among others with the safe, clean and efficient energy; the intelligent, environmentally friendly and integrated traffic; the climate change, environmental protection; and safe societies research fields. [10] Amongst the aims formulated in the latter field are:

- improvement of society's resistance against man-caused disasters;
- the research of new critical infrastructure defensive solutions;
- strengthening the fight against crime and terrorism, for example development of new criminal technology tools, new protection solutions against explosives;
- increasing cyber security, from safe information sharing methods to the development of new information safety models. [11]

2.1. ICT technologies

The ICT plays a key role in the EU's society and economy. The ICT sector gives 4,8% of the EU's economy, and it produces 25% of business research input. [12] The priorities related to the future of e-government are summed up in e-Government Action Plan, which aims to create a knowledge based, sustainable, inclusive economy. [13] The actions of e-Government Action Plan can be classified into four categories:

[2] Future and Emerging Technologies - FET

- involvement of users: services accustomed to the demands of users, improvement of transparency, involvement of citizens and companies in the formation of the regulation environment;
- internal market: barrier-free services for enterprises, mobility, implementation of cross-border services;
- the efficiency of the public sector: electronic acquisitions, faster evaluation in competitions, reduction of administrative burdens, “green” government;
- development of the electronic government and the creation of its preconditions: open specifications, helping interoperability, revision of the directive about electronic signature, mutual recognition of electronic identification and electronic verification.

Currently one of the most important EU strategic documents is the Digital Agenda for Europe (fitting with the Europe 2020 strategy), which aims to create a unified digital market, which would help Europe to take the road of an intelligent, sustainable and inclusive growth. The actions of the Digital Agenda among others:

- creating a unified digital market;
- to the field of interoperability and standards;
- strengthening trust and internet safety;
- providing high-speed and super fast internet access for everybody;
- furtherance of digital proficiency, digital skills, and digital integration. [14]

The H2020 defines these priority areas within the ICT program:

- new generation components and systems: creating developed and intelligent, energy-sufficient, and resource friendly embedded systems, components, systems;
- new generation IT: modern and safe IT systems and technologies, grid and cloud based technologies;
- future internet: software, hardware, infrastructure, technologies and services, Ubiquitous Computing, Service oriented computing, semantic web, 3D internet, Internet of Things, visual information request, smart home, smart city, etc;
- content management technology and information management: the digital content, information and communication technologies supporting culture and the creative industry, e-public administration technologies;
- developed interfaces and robots: robotics and intelligent spaces, autonomic robots, artificial intelligence;

- micro- and nanoelectronics, fotonics, and quantum technologies. [12]

Most of these, for example the ICT systems aiming energy efficiency, modern and safe IT networks, cloud based systems, the use of digital content management systems in public administration etc. also fit into the circle of technical researches aiming the operation of the state.

2.2. Information security – cyber security

Thanks to the significant forging ahead of the ICT, information safety and cyber safety became one of the most important security questions of today. The already mentioned Digital Agenda for Europe is an emphatic element of the cyber protection policy of the European Union. Amongst the seven key action areas the question of trust and safety is one of the pivotal issues.

- creating a network of groups managing computer emergencies around Europe;
- simulation of large-scale internet attacks, and testing threat mitigation strategies;
- creating a hotline-network for reporting illicit and offensive content;
- creating a cautionary platform against computer crime, or its adaptation to the Europol's system. [14]

The European Union's cyber security strategy summarizes the EU's comprehensive vision regarding the methods to efficiently prevent and fend off the vulnerability and network disturbances caused by ICT technology. The new strategy emphasizes five priorities, which also represent research priorities:

- creating resistance against cyber attacks;
- drastic suppression of IT crime;
- developing a cyber protection policy and abilities related to common safety- and protection policy;
- obtaining industrial and technological resources needed for cyber security, and lastly
- elaborating a unified, international policy for the cyber space represented by the EU, and disseminating basic EU values. [15]

The requirements expressed in this strategic document naturally assume that serious technical researches must happen in the areas of information security and cyber security in the following years, which would serve as a basis for the feasibility of strategic requirements.

All this also appear in the H2020, inside the pillars of "Societal Challenges", in the research area of secure societies. In the work program of “Secure Societies" for 2016-17 on the critical infrastructure protection and digital safety focus areas the following main research directions can be recognized:

- preventing and detecting physical and cyber threats against the critical infrastructures, responses and the mitigation of damages;
- developing safety and certification methods for reliable and safe ICT systems, tools and services;
- the cyber safety of government and council administrative ICT systems and SMEs and the ICT systems of individuals;
- developing the system level digital safety of healthcare data;
- cipher;
- handling developed cyber safety threats (ATP attacks, zero-day exploit, etc.);
- protecting personal data. [16]

2.3. Environmental security

Into the concept of environmental safety such events and processes fall that can be classified into three groups. Into the first group belong possible damages of natural origin, such as earthquakes, floods, destructive wind storms, forest fires, etc. Into the second group belong damages of technical origin, i.e. when man-made dangerous materials unexpectedly and in a large extent get out into nature, causing undesirable effects. Into the third group belong such social related events, which cause environmental damage either directly or indirectly. These events or processes can be local or regional war, migration – including war refugees – the dominance of poverty or classical economic robber management. [17]

From the unfavorable economical effects the increase of soil erosion, quality deterioration of water resources, unfavorable changes in radiation conditions, the increase of background radiation, the disruption of the temperature equilibrium, the drastic decrease of biodiversity, plant pathogens and animal pests, and the passage of illnesses from one country to another may be mentioned.

To its research and application areas belong waste management, protection of polluted settlements, species and habitats, soil science, recycling, agriculture, landscape architecture, nature protection policy, water.

The main research areas of today are:

- the social effects of environmental changes;
- today’s environmental changes, such as global warming;
- pollution and environmental damages;
- environmental effect assessment;

- reconstruction of previous environmental effects. [18]

About the issue of environmental safety narrowed down for the environment of the European Union the EC Contract states that the goal is to reach high level environmental protection. Environmental policy must take scientific facts, the environmental state of the Commission, the cost and benefit of the activities in this field of the Commission, and the economical and social state of the Commission and the given region into account. Union researches shown that the environmental tension can contribute to the emergence of serious conflicts under certain economical and social conditions. Some of the environmental factors:

- global environmental problems mean a greater danger than regional problems or problems within the country;
- it is not easy to define individual responsibility in the emergence of global environmental problems;
- four groups of environmental changes, such as degradation, pollution, shortage, bad distribution or disaster or accident can cause potential cross-border effect.

In the H2020 "Societal Challenges" pillar, in the “Climate Action, Environment, Resource Efficiency and Raw Materials” actual work program there are a great number of themes related to environmental security, and its technical aspects. Here are some of the more important research topics:

- integrated European regional climate modeling and prediction system;
- robust and overall system for the supervision of greenhouse gases;
- a million and a half year retrospection to improve the efficiency of climate prediction;
- eliminating and making the European economical coal dependency flexible for the 2030-2050 time period and beyond;
- coordinating and supporting research and innovation activities for the elimination of European coal dependency;
- new solutions for the sustainable production of raw materials;
- modern environmental surveillance systems.[19]

The LIFE program started in 1992 is the European Union’s financial tool for funding environmental protection, which Hungary joined in 2001. [20] The general goal of LIFE is to support the modernization and implementation of environmental politics and legislation. The “LIFE program 2014-2017 multiannual work program” approved by the EU’s Committee achieves the EU’s environmental protection policy trough two subroutines. These are:

- Environmental protection subroutine and

- Climate policy subroutine.

The Environmental protection subroutine contains three emphasized areas: Environment and resource efficiency, nature and biological diversity, and Environmental protection control and information. Within these it defines such thematic priorities, as water (including maritime environment), waste, resource efficiency (including soil and forests, and green and all-round economy), environment and health (including chemicals and noise), the quality of air and emissions (including urban environment), nature, biological diversity, information, increasing awareness, etc.

The subroutine of Climate policy supports the implementation of a low carbon-monoxide emission union economy resilient against the effects of climate change, strategically supports the execution of the 2020 climate change and energy package, and prepares the EU for climate policy challenges until 2030. Besides it also supports the better climate policy management on every level, including the increased inclusion of civil society, nongovernmental organizations and local personas. [21]

The safe, clean and efficient energy production is one of today’s extremely important issues, which shows a close correlation with the operation of the state. The Unites States Department of Energy formulated their related notion titled “National Electric Delivery Technologies Roadmap” after consulting 200 energy industry experts in the beginning of 2004. This document draws up the main aspects of a long-term (25 year) research-development strategy. Its point is that a new electricity system’s possible architectures suitable for the challenges of the future, and a sustainable, stable system of its structure and operation must be developed. The conclusions and suggestions of this document can be summarized as follows:

- the improvement of so called “critical technologies” is needed:
  - different capacity, efficient energy storages;
  - divided and intelligent measurement and control: intelligent measuring equipment; new, task specific data transfer architectures and protocols; new perspective protections and system rescue automatics; market dependent consumer side intervention;
  - high temperature supraconductive material and appliances based on them;
  - further development of high power appliances for the connection of the distributed energy producer and storage appliances, for the development of voltage quality, and for the more reliable automation of transmission and distribution;
- for the sake of accelerating the technological transfer, the following are needed:
  - development of new business models, the support of regulating authorities;
  - development of new university curricula, further development of the current ones;

  - further development of professional training, development of simulation software systems replicating the nature of new technologies;
- for the more efficient operation of the energy market the following are needed:
  - development of an information system suitable for collecting and forwarding large amounts of real-time data;
  - revision of law and regulation background regulating the market. [22]

The resolutions of the European Union (e.g. SET-Plan) put a great emphasis on the following topics:

- efficient integration of renewable energies in favor of reducing the dependence on carbon-based primary energy sources;
- development of so called Micro Grids in favor of avoiding system malfunctions, which are capable of forming viable islands independently as needed, then automatically reconnecting;
- the importance of the development of high level specialization and multidisciplinary education. [23]

One of the important issues of the framework program of EU H2020 is the support of energy sector researches. The work program titled "Safe, clean and efficient energy" contains many related research topics, from which some of the most important ones can be found in the following:

- recovery and recycling of waste heat energy from urban facilities to increase the efficiency of communal and individual heating and cooling systems;
- increasing the efficiency of outdated communal heating systems;
- standardized installment packages for the establishment systems providing integrated and energy efficient heating, cooling, and/or hot water utilizing renewable energies;
- new heating and cooling solution utilizing low quality heat energy sources;
- models and tools that can be used for assessing and planning the establishment of heating and cooling systems;
- assessing waste heat generated in industrial systems;
- increasing the share of renewable energies by using new generation innovation technologies, intelligent networks, integrating storage and energy systems, distribution networks;
- development of new generation bio fuel producing technologies;
- precompetitive solutions for the utilization of solar energy in industrial processes;
- demonstrating the most promising development directions in bio fuel production;
- high efficiency and flexibility power plants utilizing fossil fuel. [24]

SUMMARY AND PRELIMINARY TO PART 2

Instead of conclusions, we would only like to give a short summary here, to the end of the first part. The detailed discussion will be at the end of Part 2 (to be placed in the next journal edition).

What we have done so far is the introduction of state and governance researches running at the National University of Public Service especially with their interconnection with engineering sciences. A lot of points of common interest could be found and this first part of our paper focused on these. Findings of ongoing engineering researches and cutting edge technologies can serve as tools for the problem solving in case of many domestic and international state and governmental programs. A detailed overview has been planned to give in this paper from several areas of engineering researches. In this first part the fields of ICT technologies, information security and environmental security were introduced. The upcoming second part of the paper will cover the fields of disaster management, defense oriented technical researches, logistics and transport.

Based on the displayed international trends, in the final part we will summarize the promising technical research possibilities on certain areas at the NUPS and final conclusions will also be placed there.

References

[1] Perez, C.: Technological revolutions and techno-economic paradigms. Working Papers in Technology Governance and Economic Dynamics No. 20, Tallinn University of Technology, Tallinn, January 2009. http://hum.ttu.ee/wp/paper20.pdf (downloaded: 2016. 02. 23.)

[2] Pollitt, C.: Technological Change: A Central yet Neglected Feature of Public Administration. NISPAcee Journal of Public Administration and Policy, Volume 3, Issue 2, December 2010, pp. 31-54.

[3] Sismondo, S.: Science and Technology Studies and an Engaged Program. In Hackett, E. J.; Amsterdamska, O.; Lynch, M.; & Wajcman, J.: The handbook of science and technology studies, The MIT Press, Cambridge, 3rd edition, September 28, 2007., pp. 13-31.

[4] Wyatt, S: Technological Determinism is Dead; Long Live Technological Determinism" In Hackett, E. J.; Amsterdamska, O.; Lynch, M.; & Wajcman, J.: The handbook of science and technology studies, The MIT Press, Cambridge, 3rd edition, September 28, 2007., pp. 165-180

[5] NKE Kutatási-Fejlesztési és Innovációs Stratégia 2015-2020 (draft), NKE, 2015.

[6] Nemzeti Infokommunikációs Stratégia 2014-2020 http://www.nisz.hu/sites/default/files/u1/nemzeti_infokommunikacios_strategia_2014_2020.pdf (downloaded: 2016. 02. 23.)

[7] A Katonai Műszaki Doktori Iskola képzési terve, 2015. http://hhk.uni-nke.hu/uploads/media_items/kmdi-kepzesi-terv-3.original.pdf (downloaded: 2016. 02. 23.)

[8] 1999. évi LXXIV. törvény a katasztrófák elleni védekezés irányításáról, szervezetéről és a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

[9] 2011. évi CXXVI II. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról.

[10] Horizont 2020 III. Társadalmi kihívások http://www.h2020.gov.hu/iii-tarsadalmi-kihivasok (downloaded: 2016. 02. 23.)

[11] Secure societies – Protecting freedom and security of Europe and its citizens. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens (downloaded: 2016. 02. 23.)

[12] Horizont 2020 Információs és Kommunikációs Technológiák http://www.h2020.gov.hu/ii-ipari-vezeto-szerep/informacios/informacios (downloaded: 2016. 02. 23.)

[13] COM(2006) 173 final i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, Brussels, 25.04.2006. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0173&from=EN (downloaded: 2016. 02. 23.)

[14] Dr. Négyesi Imre: Informatikai rendszerek és alkalmazások a védelmi szférában (Dunaújvárosi Főiskola Közleményei (2010), XXXI. évfolyam, ISSN 1586-8567);

[15] COM (2010) 2045 Az európai digitális menetrend. Európai Bizottság, Brüsszel, 2010.5.19. http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52010DC0245&from=HU (downloaded: 2016. 02. 23.)

[16] JOIN(2013) 1 final Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, Brussels, 7.2.2013 http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 (downloaded: 2016. 02. 23.)

[17] Horizon 2020 Work Programme 2016 - 2017. 14. Secure societies – Protecting freedom and security of Europe and its citizens. http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf (downloaded: 2016. 02. 23.)

[18] Dr. Halász L., Dr. Földi L.: Környezetbiztonság, NKE, Budapest, 2014. p. 141, ISBN 978-615-5305-97-9, https://opac.uni-nke.hu/webview?infile=&sobj=9279&source=webvd&cgimime=application%2Fpdf%0D%0A (downloaded: 2016. 02. 23.)

[19] Dr. Négyesi Imre: Informatikai rendszerek oktatása a katasztrófavédelmi szakirányon (Hadmérnök on-line, V. évfolyam (2010) 2. szám, 25-40. oldal, ISSN 1788-1919).

[20] Krajnyák Z., Nagy Zs., Zsiros A.: Az ember tevékenységének következményei napjainkban, Nyíregyházi Főiskola, Környezettudományi Tanszék http://www.nyf.hu/others/html/kornyezettud/oktatoanyag/segedlet/az_ember_es_korny/ember_tevek_napjainkban/emberi_tev_napjainkban_index.htm (downloaded: 2016. 02. 23.)

[21] Horizon 2020 Work Programme 2016 – 2017. 12. Climate action, environment, resource efficiency and raw materials.

http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-climate_en.pdf (downloaded: 2016. 02. 23.)

[22] The LIFE Program http://ec.europa.eu/environment/life/about/index.htm (downloaded: 2016. 02. 23.)

[23] 2014/203/EU A Bizottság végrehajtási határozata a LIFE program 2014–2017. évi többéves munkaprogramjának elfogadásáról (2014. március 19.) http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32014D0203&from=EN (downloaded: 2016. 02. 23.)

[24] Basic Energy Sciences Summary Report. U.S. Department of Energy, 2014. http://science.energy.gov/~/media/bes/pdf/reports/files/BES2014SR_rpt.pdf (downloaded: 2016. 02. 23.)

[25] Dr. Négyesi Imre: COTS rendszerek alkalmazási lehetőségeinek vizsgálata (Hadtudományi szemle on-line, IV. évfolyam (2011) 4. szám, 111-116. oldal, HU ISSN 2060-0437)

[26] Bertoldi, P., Atanasiu B.: Effective Policies for Improving Energy Efficiency in Buildings. Krakow, Poland, 12-14 September 2007. Proceedings of the JRC Workshop on Scientific Technical Reference System on Renewable Energy & Use Efficiency. European Commission Joint Research Centre Institute for Environment and Sustainability http://www.eurosfaire.prd.fr/7pc/doc/1278343470_lbna23548enc_002.pdf (downloaded: 2016. 02. 23.)

[27] Horizon 2020 Work Programme 2016 – 2017. 10. Secure, Clean and Efficient Energy. http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-energy_en.pdf (downloaded: 2016. 02. 23.)

[28] Négyesi Imre: DIE ÜBERPRÜFUNG DER VORAUSSETZUNGEN VON COTS SYSTEMEN (COTS RENDSZEREK KÖVETELMÉNYEINEK VIZSGÁLATA) (Hadmérnök on-line, VII. évfolyam (2012) 2. szám, 371-376. oldal, ISSN 1788-1919).

Developments of Identification and Trust Services in Public Administration through eIDAS

Otto Izso[1], Dr. Imre Négyesi[2]

1: Doctoral School of Public Administration Sciences; NUPS, Hungary

2: National University of Public Service, Hungary

Abstract

From July 1, 2016, the EU eSignatures Directive (1999/93/EC), was replaced by Regulation (EU) No. 910/2014 on electronic identification and trust services called the eIDAS regulation. eIDAS is the result of the European Union's Digital Agenda aimed to drive digital growth in the Union. As an EU regulation, the eIDAS is directly applicable law in all twenty-eight EU member states and in the European Economic Area. eIDAS wants to ensure that secure electronic identification and authentication is possible for cross-border online services offered by member states and electronic signatures will have the same legal weight as their physical counterparts. The eIDAS regulation was adopted to facilitate seamless digital transactions for individuals, businesses, and public administrations across countries within the European Union in two areas: electronic identification services and trust services. The new regulation expected to foster a climate of trust when it comes to online and digital transactions in the EU.

Keywords: eIDAS, Public Administration, Identification and Trust Services

Introduction

From July 1, 2016, the EU eSignatures Directive (1999/93/EC), was replaced by Regulation (EU) No. 910/2014 on electronic identification and trust services called the eIDAS regulation. eIDAS is the result of the European Union's Digital Agenda[3] aimed to drive digital growth in the Union. As an EU regulation, the eIDAS is directly applicable law in all twenty-eight EU member states and in the European Economic Area. eIDAS wants to ensure that secure electronic identification and authentication is possible for cross-border online services offered by member states and electronic signatures will have the same legal weight as their physical counterparts. The eIDAS regulation was adopted to facilitate seamless digital transactions for individuals, businesses, and public administrations across countries within the European Union in two areas: electronic identification services and trust services. The new regulation expected to foster a climate of trust when it comes to online and digital transactions in the EU.

eIDAS addresses *interoperability* and *transparency* requirements. Compliance with the interoperability common architecture defined by eIDAS[4] enables member states to deliver a framework that will recognize eIDs issued by any of the other member states. With regards to transparency eIDAS requires member states to maintain and publish a list of qualified trust providers and the specific trust services provided by them. A trust service provider must appear on this list to be a qualified. Trust services include digital signatures, time stamping, electronic seal, registered electronic delivery, and website authentication.

According to the eIDAS regulation electronic signatures are classified in the following three categories: simple, advances, and qualified. A *simple electronic signature* is the equivalent of a written signature. Some examples of a simple signatures are a typed name at the bottom of an e-mail, a scanned hand-written signature in a PDF file, or clicking an "I accept" button on a web page. *Advanced electronic signatures* are produced using encryption and can be used across member states. It must have a unique linking capability of identifying the signatory and it must be linked to the signed data in a way that any change in it is detectable. *Qualified electronic signatures* are advanced electronic signatures backed a qualified certificate issued by a trust service provider whose credentials appear in the EU trusted list. Advanced and qualified electronic signatures enable automated processes, digital proof of signatures, non-repudiation.

[3] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Agenda for Europe

[4] "eIDAS – Interoperability Architecture" v. 1.00; November 6, 2015; https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

The Implementing Acts

The European Commission also adopted eight implementing acts related to the eIDAS regulation in 2015 and 2016. Four of them concern electronic identification and the other four relate to electronic trust services:

Implementing acts concerning electronic identification:

- Commission Implementing Decision (EU) 2015/296[5] of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014
- Commission Implementing Regulation (EU) 2015/1501[6] of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014
- Commission Implementing Regulation (EU) 2015/1502[7] of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014
- Commission Implementing Decision (EU) 2015/1984[8] of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014

Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014. Member states must work together to ensure interoperable and secure electronic identification systems. The decision also addresses information-sharing and creates a cooperation network supervised by the EC and made up of the member states' representatives and the countries of the EEA.[9]

Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 This regulation lays the foundation for a technical platform delivering an interoperability interface amongst the different eID systems.[10] Article 11 specifies the minimum set of data for both natural and legal persons to be used in a cross-border context.

To assist member states with the their own eIDAS compliant implementation, technical specifications are developed by the European Commission with assistance from the eIDAS Expert Group. The technical specifications supporting Commission Implementing Regulation (EU) 2015/1501 are not static as they are subject to further development. To date, there had been two releases (26/11/2016;

[5] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d0296_en_txt.pdf
[6] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1501_en_txt.pdf
[7] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1502_en_txt.pdf
[8] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1984_en_txt.pdf
[9] www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html
[10] www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html

16/12/2016). The technical specifications cover eIDAS Message Format[11], Interoperability Architecture[12], Crypto Requirements for the eIDAS Interoperability Framework[13], and SAML Attribute Profile[14].

Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014

This implementing regulation establishes minimum technical specifications and procedures for low, substantial and high assurance levels for electronic identification. [15]

Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014

This implementing decision sets out the process for notifying the European Commission of an electronic identification system including the description of the technical specifications of the system, definition and justification of the assurance levels. Notification is followed by a peer review of the system by the other member states.[16]

Electronic Trust services:

- Commission Implementing Regulation (EU) 2015/806[17] of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services
- Commission Implementing Decision (EU) 2015/1505[18] of 8 September 2015 laying down technical specifications and formats relating to trusted lists
- Commission Implementing Decision (EU) 2015/1506[19] of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies

[11] https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eIDAS%20Message%20Format_v1.1-2.pdf?version=1&modificationDate=1497252919575&api=v2

[12] https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eidas_interoperability_architecture_v1.00.pdf?version=1&modificationDate=1497252919857&api=v2

[13] https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eidas_-_crypto_requirements_for_the_eidas_interoperability_framework_v1.0.pdf?version=1&modificationDate=1497252920224&api=v2

[14]www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html
https://ec.europa.eu/cefdigital/wiki/download/attachments/46992719/eIDAS%20SAML%20Attribute%20Profile%20v1.1_2.pdf?version=1&modificationDate=1497252920100&api=v2

[15]www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html

[16]www.personalausweisportal.de/EN/Government/eIDAS_Regulation/Regulation_Implementing_Acts/regulation_implementing_actss_node.html

[17] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r0806_en_txt.pdf

[18] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1505_en_txt.pdf

[19] https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1506_en_txt.pdf

- Commission Implementing Decision (EU)2016/650[20] of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices

The Standards

European Telecommunications Standards Institute (ETSI)[21] supports eIDAS through the establishment of necessary standards in six functional areas:

1. Signature creation and validation
2. Signature creation and other related devices
3. Cryptographic suites
4. Trust service providers supporting digital signatures and related services
5. Trust application service providers
6. Trust service status lists providers

ETSI issues the following document types required for standardization:

- Guidance
- Policy & security requirements
- Technical specifications
- Conformity assessment
- Testing conformance & interoperability

Electronic Identification Card (EIC)[22]

Each period of the European EIC evolution can be characterized by a concept, functional user group, European interoperability idea and security solutions.

Following the adoption of the EU eSignatures Directive (1999/93/EC), the period of key cards can be placed between 2002 and 2007. The electronic identification cards function as a key to access and manage server based personal data. Primary example of key card is the Estonian national identity card (see more detail about this later). The Estonian national identity card functions as an analog personal identification document, but is also required for accessing electronic public services. The built-in chip allows digital identification of a person and the use of electronic signatures.

After the launch of the European Citizen Card concept and standards in 2008/2009 support for electronic signature on contact chip cards strengthened. Data for personal identification appeared in

[20] https://ec.europa.eu/futurium/en/system/files/ged/celex_32016d0650_en_txt.pdf

[21] Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures: overview (TR 119 100 v1.1.1); http://www.etsi.org/deliver/etsi_tr/119100_119199/119100/01.01.01_60/tr_119100v010101p.pdf

[22] "Az új, tároló elemet tartalmazó személyazonosító igazolvány bevezetésével összefüggő változások", SZAKMAI OKTATÓANYAG, 2015. p. 5-6

the memory of the chip and security features and data protection had undergone substantial advances. Belgium and Portugal (based on the Belgian card) cards are considered the initiators of this area.

The German personal identification card (nPA) opened a new area in 2010. The document was the first to include a contactless chip and serve as a travel document, electronic identification and electronic signature.

eID Schemes

Country	Name of the eID scheme	Type	Status
Austria	National Citizen ID	Multimean	In use
Belgium	National ID	Smartcard	In use
Bulgaria	National ID	Smartcard	In development
Croatia	e-Citizen	Multimean	In use
Cyprus	ARIADNI National ID	Login TBC	In use In development
Czech Republic	National ID mojeID	Smartcard Login	In development In use
Denmark	NemID	Login	In use
Estonia	National ID	Multimean	In use
Finland	FINeID TUPAS	Certificates Mobile	In use In use
France	FranceConnect	Login	In development
Germany	National ID	Smartcard	In use
Greece	ERMIS portal National ID	Login Smartcard	In use In development
Hungary	eSzemelyi	Smartcard	In use
Ireland	MyGovID	Login	In use
Italy	SPID National ID	Multimean Smartcard	In use In development
Latvia	eParaksts	Smartcard	In use
Lithuania	National ID	Smartcard	In use
Luxembourg	National ID LuxTrust	Smartcard Multimean	In use In use
Malta	National eID	Smartcard	In use
Netherlands	DigID eHerkenning Federation: Idensys, iDIN, DigID	Login Login Multimean	In use In use In development
Poland	National ID	Smartcard	In development
Portugal	Cartão do Cidadão Chave Móvel Digital	Smartcard Mobile	In use In use
Romania	National ID	Smartcard	In development
Slovakia	National ID	Smartcard	In use
Slovenia	eUprava	Certificates	In use
Spain	National ID Various* Cl@ve	Smartcard Certificates Login	In use In use In use
Sweden	Bank ID e-Legitimation (Telia)	Multimean Multimean	In use In use
United Kingdom	GOV.UK VERIFY	Multimean	In use

Table 1. Status of eIDs in Europe – Source: CEF Digital/Country overview; https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+Overview+-+eID

STATUS OF eIDs

The electronic identification schemes already in use or under development in Europe (see Table1.) illustrate that eIDAS allows member states flexibility to implement their choice of electronic identification if it complies with specifications set out by eIDAS. Smart card/chip enabled electronic identification cards are the preferred choice with sixteen of the member states opting for this option. Ten of these countries already use the smart card enabled ID card and another six are under development. eIDAS also does not require member states to introduce electronic identification as a mandatory/national identification document.

Germany was the first country to notify in July 2017. The notification process refers to the selection, peer review and official addition of national eID schemes to the eIDAS Network. The German electronic identification card (Der Personalausweis) enables citizens to access a variety of services from municipal, state and federal public administration system, to registering for university courses, and logging onto various insurance, financial and other services' websites. The card can also function as a travel card on Deutche Bahn. The biometric identifiers are restricted for use by the police and in border control, and are not available for online purposes.[23]

One of the most digitally developed countries in the world, ***Estonia*** has extensive experience with electronic identification. Estonia introduced electronic national identity cards in 2002 and currently has nearly 1.3 million national eIDs in force. In addition to serve as a traditional personal identification document, the eID comes with several functionalities, including:

- online access (login) to governmental institutions, public services, e-business services, banks and various other e-services in Estonia
- sign document electronically
- encrypt/decrypt documents
- i-voting
- e-prescriptions
- customer/loyalty card

Digi-ID is a stripped-down version of the above described national ID without the analog personal identification features, but with very similar electronic functionalities.

It is also possible to obtain a mobile-id with many of the same digital functionalities as the national ID, but without the need for a card reader.

Estonia also offers e-Residency to non-Estonians with the primary purpose of running location independent EU businesses online. [24]

[23] www.personalausweisportal.de/EN/Home/home_node.html
[24] www.id.ee/?lang=en

Emerging Security Risk[25]

Chip based electronic identification cards are considered very secure. However, Estonia had to block the certificates some 760 000 cards early November 2017 as a pre-emptive step based on a threat assessment by the authorities. As international cybercrime networks had become aware of a security flaw, the Estonian government decided to block the impacted certificates to prevent the possibility of e-identity theft.

The Estonian government understood that the e-state cannot function without unquestionable trust and delay would have increased the risk of actual identity theft which in turn would have raised serious questions in citizens concerning their trust in the e-state.

CER Estonia also posted a warning about the possibility that cybercriminals may attempt to exploit this situation and asked the public not to respond to any messages offering assistance with the ID card update, but instead forward them to CERT EE.[26]

While the security flaw identified (ROCA vulnerability) impacted only certain cards issued between specific dates, it still highlights the issue that digital identifications are not immune to flaws and when corrupted it may lead to a large-scale problem e.g. certificates on over 50% of the active Estonian national ID cards had to be blocked.

Hungary passed a number of legislations, including the Act CCXXII of 2015 regarding the electronic administration and general rules for trust services[27], 24/2016. (VI. 30.) of the Minister of Interior, providers of trust services and detailed requirements[28], 26/2016. (VI. 30.) of the Minister of Interior, trust, and records kept by the content of the notifications relating to the provision of trust services[29] and by the 414/2015. (XII. 23.) Government Decree on the Issuance of an Identity Card and the Single Facsimile and Signature Records Rules[30] to ensure regulatory alignment with eIDAS.

Hungary issues electronic personal identification cards since January 1, 2016. The cardholder's name, place of birth, date of birth, citizenship, mother's maiden name, sex, photo, signature, expiration date of the ID card, document identification number, date of issuance, and issuing authority are printed on

[25] Press Release: "Estonia will block the certificates of 760 000 ID cards as of the evening of 3 November"; November 2, 2017; https://www.id.ee/?id=30610&read=38341

[26] https://twitter.com/CERT_EE/status/926475950883328000

[27] 2015. évi CCXXII. törvény Törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól, MK 2015/202. (XII. 23.) p. 26809-26859

[28] 24/2016. (VI. 30.) BM rendelet Rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről; MK 2016/95. (VI. 30.) p. 7675- 7687

[29] 26/2016. (VI. 30.) BM rendelet Rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről; MK 2016/95. (VI. 30.) p. 7689 - 7694

[30] 414/2015. (XII. 23.) Korm. rendelet a személyazonosító igazolvány kiadása és az egységes arcképmás- és aláírás-felvételezés szabályairól, MK 2015/202. (XII. 23.) p. 26992- 27013

the card. The card also has an ICAO standard machine-readable zone (MRZ) which includes the key data elements required for personal identification.[31]

The chip imbedded card has four key electronic functions. The electronic travel document function (ePASS) allows citizens to use electronic gate entry system and other automatic electronic passenger entry systems where available - primarily at airports/ports in the Schengen-zone. The ePASS function also supports certain law enforcement task by making identification of a person easier and more secure. The electronic identification function (eID) allows citizens access to eGovernment and on-line public administration systems more effectively and at a higher security level than previous access methods (e.g. username/password). Full eIDAS compatibility of the Hungarian eID will also enable Hungarian citizens to access these systems in other EU countries as the cross-border capabilities rolled out in the member states. Access to and use of the social security number (TAJ) and tax identification number stored in the chip are also part of the eID function. The electronic signature function (eSIGN) is capable providing qualified electronic signatures with the same legal weight as their physical counterparts in accordance with Act. XXXV. 2001. Although the Hungarian electronic national ID is not issued in the National Unified Card System (NEK), the other electronic services function (eNEK) allows the card holder to access on-line NEK services. Other functions also include the ability to use electronic public transportation services (e.g. eTicket) given that these future systems are compatible with the NEK system. The range of additional electronic/on-line services accessible with the electronic national ID is expected to grow substantially in the future.

	2016 H1	**Proportion of applicants as a ratio to total eligible**	**2017 H1**	**Proportion of applicants as a ratio to total eligible**
Cards w/o chip	58,545	74.3%	63,949	86.3%
Fingerprint	324,649	56.7%	265,564	49.0%
e-Signature	46,701	8.5%	30,550	5.9%
Emergency Contact Number			187,956	28.1%

Table 2. Number of applications and the ratio of applications among total eligible for selected key functions and services of the Hungarian eID. Author's own creation. Source: Elektronikus közszolgáltatásokat és ügyfélszolgálati tevékenységet összefoglaló monitoring jelentés - 2017. I. félév

[31] "Az új, tároló elemet tartalmazó személyazonosító igazolvány bevezetésével összefüggő változások", SZAKMAI OKTATÓANYAG, 2015. p. 8

Analysis of the take up of the new electronic functions provided by the Hungarian eID card reveals, that most citizens over the age of sixty-five elect to receive the identification document without chip imbedded. Primary reason appears to be the fact that citizens over the age of sixty-five are allowed by law to receive a no chip card with no expiration date. However, it should be noted that while the ratio of no-chip cards appears to be very high among the eligible age group, overall these cards make up a lesser, but still sizable 9.6% of total new applications.

Recording of cardholder's fingerprint on the chip has declined versus 2016 and is slightly below fifty percent. The likely primary reason for this citizens' concern for privacy and lack of understanding how fingerprint data effect utility of the card either way. The very low take-up (5.9% vs 8.5% in H1 2017 vs. H1 2016) appears to be a strong indicator that applicants do not understand and see the benefit of having e-signing capability in their hands which also reflects the fact that the use of e-signatures is not wide spread in Hungary.

As one of the objectives of the introduction of eIDs and eSignatures is providing citizens with convenient time-saving on-line remote access to public services, it is important to consider the country's starting point in terms of eGovernment and digital readiness. According to the most resent (2017) Digital Economy and Society Index (DESI), Hungary ranks 21th out of the EU 28 and belongs to the Low Performing Cluster of countries together with Romania, Bulgaria, Greece, Italy, Croatia, Poland, Cyprus, and Slovakia.

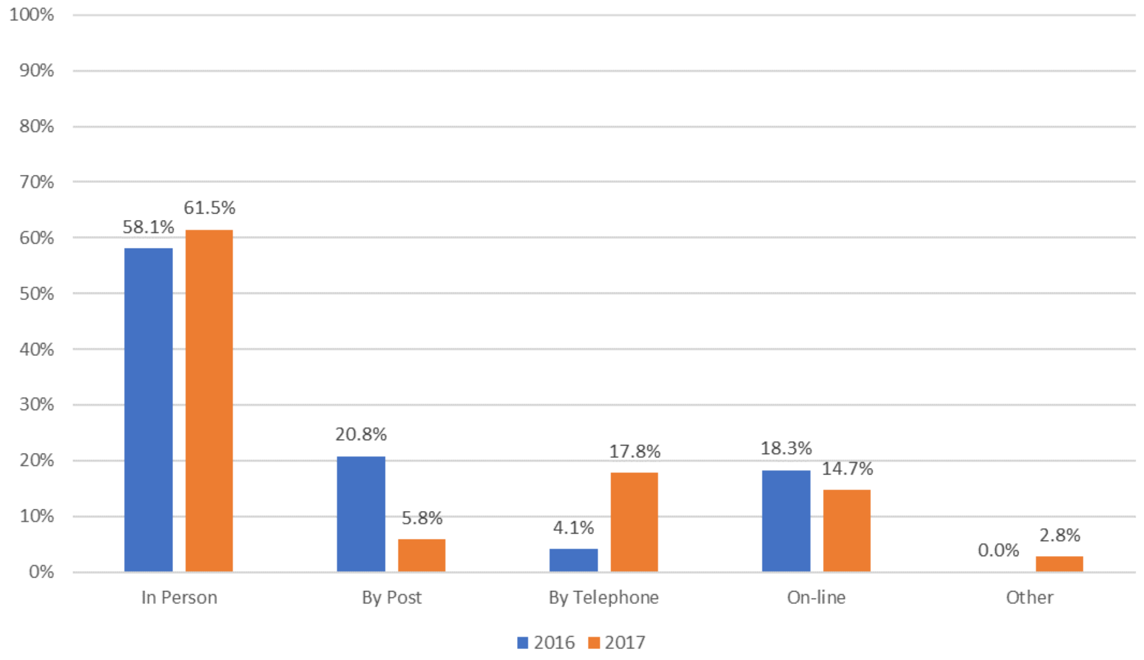

Chart 1. Utilization of public administration channels available. Author's own creation, Source: Jó Állam Jelentés 2017

The 2017 Good State and Governance Report examined through which channels the Hungarian public access public administration services (see chart 1). The survey had found that despite the progress made increasing online accessibility of public services, the clear majority of public administration services are still conducted off-line/in person (61.5%, 2017), usage of postal services has dropped considerably compared to the prior year (5.8%, 2017 vs 20.8%, 2016), and it appears that this drop indicated a shift in client preference conducting public administration services by telephone. Surprisingly, share of online/digital public services have also declined from just above 18% in 2016 to below 15% in 2017. The report identifies many factors contributing to this trend. The primary reason cited by the report is that most cases cannot be fully completed online. In addition, limited digital accessibility and lack competence; lack of trust in online customer service; impersonal nature of the online world and preference of face-to-face interaction, lack of clarity what, where and how can be done, time consuming to figure out what should be done, and too complicated instructions are some of the other key reasons identified by the report.

The report provides the following recommendations which should be consider in order to increase the share of higher value added online public services in client interactions.

- Development of comprehensive strategy to move clients to online channels and stop parallel development of all off-line channels
- Mandatory, strong motivation to move clients to online channels, instead of the voluntary migration based on perceived benefits
- Education and service marketing to combat competency and trust gaps

Conlcusion

The European Union eGovernment Action Plan 2016-2020 sets out an ambitious vision to deliver ". . . open, efficient and inclusive, providing borderless, personalised, user-friendly, end-to-end digital public services to all citizens and businesses in the EU" by 2020. It also sets the principles to be observed by the initiatives designed to accelerate the digital transformation of European governments. Public administrations should be digital by default, should ask for the same information only once, should be inclusive and accessible to all regardless of age or disability. In addition, openness and transparency, cross-borders access and interoperability of digital public services together with trustworthiness and security are the key principles to ensure trust and take up of electronic public services. eIDAS enabled electronic identification and trust services are important components of delivering this strategy.

Education of the public concerning new developments in eGovernment/electronic public administration is also a key factor of success. Informing citizens of the possible current and expected future use of eID functionalities should gradually improve the take-up of the new electronic functionalities such as e-signature. Completing the digital transformation of public administration services and engaging the private sector in developing new ways of utilising the electronic functions (e.g. financial services, public/private transport, etc.) of the eID should also drive up interest. While electronic identification card and e-signatures functionalities imbedded in them are here to stay, mobile and smart device technology are also key areas of focus given the wide use of these devices in Europe. Many of the member states already have electronic identification and signature functionalities on mobile/smart devices (see Table 1.)

References

Dumortier, Jos. "Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, July 1, 2016.

European Union: Regulation EU No 910/2014 of the European Parliament and of the Council, 23 July 2014. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014R0910&from=EN

European Union: "eIDAS – Interoperability Architecture" v. 1.00; November 6, 2015; https://joinup.ec.europa.eu/sites/default/files/document/2015-11/eidas_interoperability_architecture_v1.00.pdf

European Union: Commission Implementing Decision (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of Regulation (EU) No 910/2014; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d0296_en_txt.pdf

European Union: Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1501_en_txt.pdf

European Union: Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r1502_en_txt.pdf

European Union: Commission Implementing Decision (EU) 2015/1984 of 3 November 2015 defining the circumstances, formats and procedures of notification pursuant to Article 9(5) of Regulation (EU) No 910/2014; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1984_en_txt.pdf

European Union: Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015r0806_en_txt.pdf

European Union: Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1505_en_txt.pdf

European Union: Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies; https://ec.europa.eu/futurium/en/system/files/ged/celex_32015d1506_en_txt.pdf

European Union: Commission Implementing Decision (EU)2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices; https://ec.europa.eu/futurium/en/system/files/ged/celex_32016d0650_en_txt.pdf

Elektronikus közszolgáltatásokat és ügyfélszolgálati tevékenységet összefoglaló monitoring jelentés - 2017. I. félév, Belügyminisztérium - Informatikai Helyettes Államtitkárság,

Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben I. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 110-121. oldal, ISSN 1417-7323);

Négyesi Imre: Az elektronikus aláírás lehetőségei a Magyar Honvédségben II. (Nemzetvédelmi Egyetemi Közlemények, 11. évfolyam/3. szám (2007), 122-137. oldal, ISSN 1417-7323);

Kaiser et. al, Jó Állam Jelentés 2017, Dialóg Campus Kiadó, 2017

Leitold, Herbert. "Challenges of eID Interoperability: The STORK Project." In Privacy and Identity Management for Life, 144–50. IFIP Advances in Information and Communication Technology. Springer, Berlin, Heidelberg, 2010.

Török, Rikk: New methods to protect our network systems; AMERICAN JOURNAL OF RESEARCH EDUCATION AND DEVELOPMENT 2017:(1) pp. 4-16. (2017) ISSN 2471-9986

Press Release: "Estonia will block the certificates of 760 000 ID cards as of the evening of 3 November"; November 2, 2017; https://www.id.ee/?id=30610&read=38341

Tsakalakis, Niko, Kieron O'Hara, and Sophie Stalla-Bourdillon. "Identity Assurance in the UK: Technical Implementation and Legal Implications Under the eIDAS Regulation." In Proceedings of the 8th ACM Conference on Web Science, 55–65. WebSci '16. New York, NY, USA: ACM, 2016.

RED

7234 5610 33

ISSN 7234561-6