Capek, Jan; Ritschelova, Iva

Conference Paper

Regional E-Government - Some Problems With Data Sharing

46th Congress of the European Regional Science Association: "Enlargement, Southern Europe and the Mediterranean", August 30th - September 3rd, 2006, Volos, Greece

Provided in Cooperation with:
European Regional Science Association (ERSA)

Suggested Citation: Capek, Jan; Ritschelova, Iva (2006) : Regional E-Government - Some Problems With Data Sharing, 46th Congress of the European Regional Science Association: "Enlargement, Southern Europe and the Mediterranean", August 30th - September 3rd, 2006, Volos, Greece, European Regional Science Association (ERSA), Louvain-la-Neuve

This Version is available at:
https://hdl.handle.net/10419/118334

Regional E-Government – some problems with data sharing

Jan Čapek, Iva Ritschelova

Abstract

The e-government should start with electronic collaboration of governmental departments. Several services, like email, video conference, discussion forums, use of shared documents, etc. should be supported for assisting the efficient and productive collaboration of remote governmental departments. Since the functionality of the provided services is well known, no detailed description of each service phase is provided. The services for citizens are offered through so called governmental portals. The typical use of a governmental portal is to provide information to the citizens and to support several types of citizen–government transactions (e.g. issuing birth certificates, submitting tax forms, conducting electronic payments, etc.).

Key Words: e-government, portals, kiosks, information systems, security.

1. Introduction

Electronic government (e-government), the ability for government to provide access to services and information twenty-four hours a day, seven days a week, is an emerging force today. Government is turning attention and resources to providing information and services on-line, exploring digital democracy, and using technology for economic development. As a result, government service will be revolutionized as we progress into the Digital Age. In this new age, good government is accessible government. Good government correlates to immediate access to pertinent information. Good government is faster, cheaper and more efficient.

In preparing for e-government, local governments should set strategic goals and objectives [Hauer at all. 2002]. As part of their strategic thinking, they should decide which local services are suitable for on-line delivery. They also need to determine whether they have access to the technology, expertise, and funding that e-government requires over the long term. Local governments with multiple departments need to coordinate Web-related activities. From the beginning, local governments should identify the potential users of their Web sites and understand what they need. To benefit from others' expertise and to share resources, local governments considering e-government should evaluate similar government Web sites and learn from others. All these activities are connected into information systems.

Under the words "information systems" one can imagine computers, communication facilities, computer and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance.

It is well known that security of information systems, which is now be very important, is the protection of availability, confidentiality, accountability and integrity.

Confidentiality – the ability to contain information to those unauthorized to view and to protect against the disclosure of information where it could be damaging. This would

include keeping information private or secret. Confidentiality can be obtained by keeping information secure and preventing unauthorized access to such information.

Integrity – the quality of information that identifies how closely the data represent reality. This is the ability to keep information from being changed by unauthorized users and that the information is complete and unchanged. Unauthorized modification of log files or getting a virus that makes changes to files is a form of an integrity attack.

Availability – goes hand-in-hand with confidentiality and integrity. Availability is the ability to provide authorized users information and/or functionalities when it is requested or needed. A power outage or viruses that crash a computer system are some examples of an availability attack.

Accountability – the ability to trace an action to a unique entity. This would include keeping up all the performed actions. An audit trail is an example to enforce the accountability requirement.

Notice that the accountability security service is renamed. The term accountability is used, because it is a broader and more generic definition. Furthermore availability is added to the security services, this is done, because in many situations the availability can be seen as security service as well. Besides Stallings [Stall, 2003] also asserted that availability is considered as a security service by many other persons and models.

2. Portals

The interface between clients and the government is usually made through portal. It will be accessed through Internet-based technologies, use websites to bring information together and a gateway to provide a common interface to the back-office systems operated by government departments and agencies. The local government portal will also present publicly available information.
Within the Czech Republic are many portals of local authorities (for example, from towns to municipalities, from regions and districts to small land users, from business private sector portal to travel agency). In the last days the local governments are try merge some of this portal together.
A portal may offer the client facilities to personalise the way they view the site [Hauer at all. 2002]. This will allow the site designers to bring to the attention of the client new and changing content that the client has labelled interesting to them. This type of personalisation can be based around ‘life events’, such as I’m Having a Baby or I’m Moving House so that content (including advertising) and transactions relevant to these events could be displayed to the client. Such transactions may require processing by more than one government department.

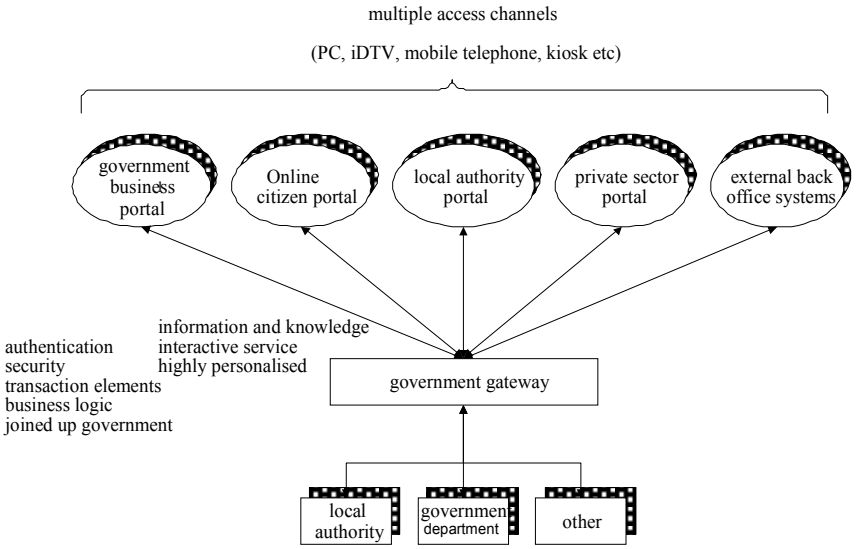


Figure 1 Portal and government gateway possible architecture

3. Government gateway

The government gateway provides the bridge between the various portals and external systems operated by government departments, local authorities and private sector service providers. It provides appropriate common security services, including client authentication, confidentiality and privacy.

Once a client has been authenticated, the government gateway forwards information between the client and appropriate government systems. It co-ordinates transactions on government systems on behalf of the client to support 'joined-up' government services covering a number of government departments and agencies (for example, the gateway would co-ordinate a change of address function).

The government gateway also provides a secure messaging facility to allow government to communicate with the client. This permits, for example, a government department to communicate with a client as part of the processing carried out.

3.1 Access to information

Citizens can access to the information offered by e-government by their home computer through Internet or by mobile device or through the information kiosks.

The information kiosks, or public access kiosks, are located in public thoroughfares, shopping malls, airports, railways stations and other locations as a substitute for, or to complement, customer service through a human service agent. In contrast to the other public access information arena, the Web accessed in the home or office, kiosks have received little media, professional or academic attention. Early kiosks, such as those reviewed by Rowley [Row1995] were typically uninteresting boxes with relatively simple interfaces, designed specially to allow customers to conduct a simple transaction, such as placing an order, or locating a specific item of information, such as a recipe or a repayment rate for a mortgage Slack & Rowley [Slack at all. 2002]. The kiosks that are now making an appearance represent a significant change of perspective on the role and nature of kiosks. These 21st century kiosks, described in [Smith1997], [Slack at all. 2002] as Kiosks 21, support multiple functions including most or all of: information provision, interaction between user and consumer to support the customisation of information, transactions (such as ticket purchase), and

relationship building through loyalty schemes or other communication opportunities. They full the four functions of kiosks described by Rowley and Slack (2000): information provision/promotion, interaction, transaction and relationships. Most significantly, Kiosks 21 represent a shift from task focus to customer focus in kiosk design. Instead of being designed to allow a customer to complete a single task, or set of closely related tasks, the kiosks offer a range of information and services tailored to the 'customer in context'. Thus, a kiosk in a shopping centre focuses on shopping-related transactions, and information, whilst a kiosk in a hotel lobby provides travel and tourist information (often with several language options) appropriate to the location of the hotel. This transition to multi-functionality and the creation of a complete support service for the 'customer in context' necessitates strategic collaboration in the provision of the information and services that can be accessed through the kiosk.

Early kiosks had very simple touch screen interfaces in which customers selected options by touching one of a number of buttons, and thereby navigated their way through the limited number of screens available for display. Kiosks 21 offer Windows or Web type functionality that includes scroll bars, pointer, hyperlinks, data entry forms, drop down lists and animation, which make for a more complex interface. This switch to more complex interfaces has been driven by:

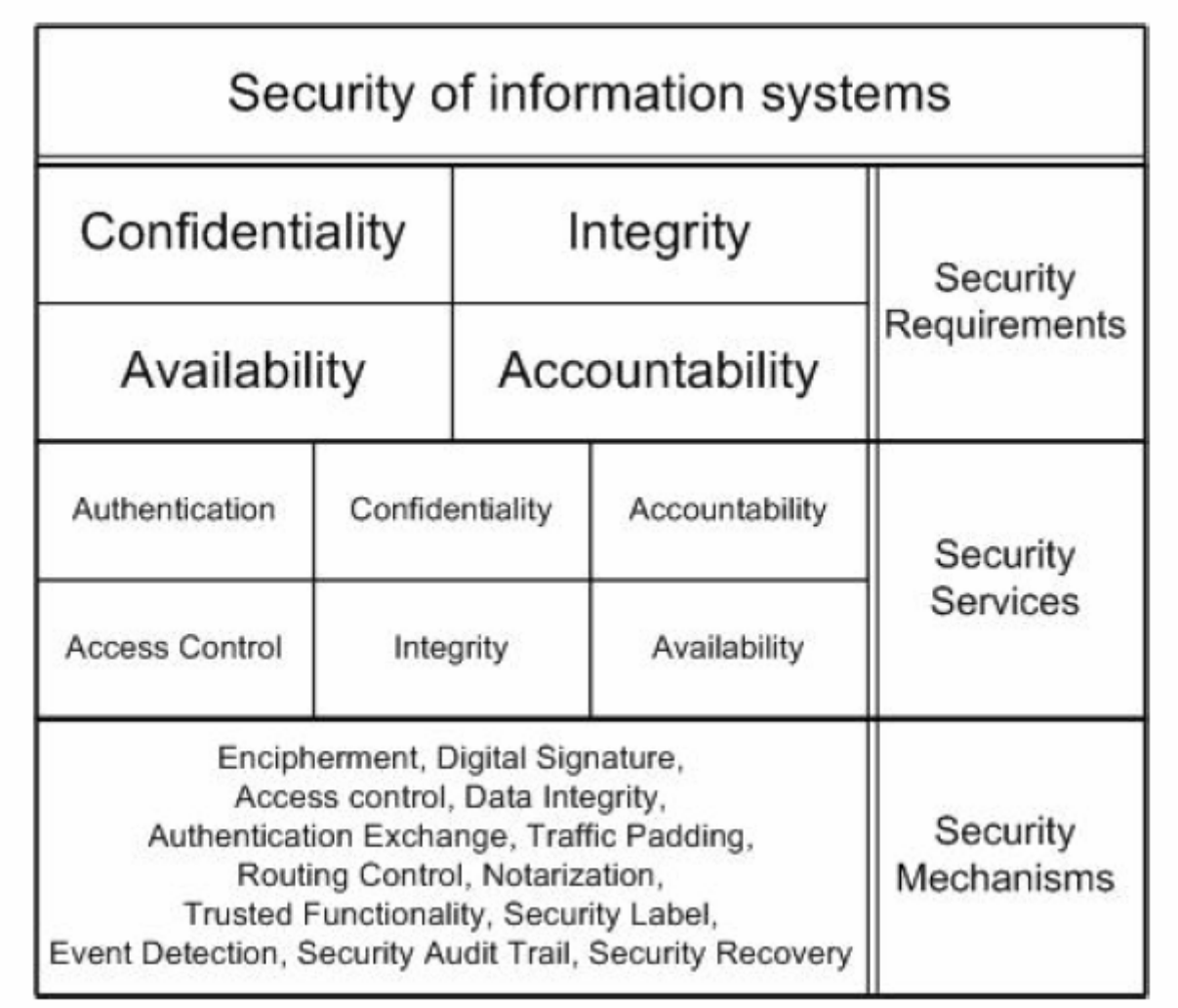
- Task or function with the shift from task completion to customer service delivery, kiosks are designed to support a wider range of activities, some of which are relatively complex, and include information retrieval and commercial transactions.
- Information source when web pages are displayed this increases the detail on the screen, and also produces pages that need to be scrolled because they exceed the screen size.
- Technology associated primarily with the connectivity offered by the internet, which provides access to real time information, and communication links, such as are available through e-mail.
- User Kiosks 21 assume a computer literate user who understands a web page format, and is prepared to navigate a larger and more complex InfoBase.

Finally, the location and physical design of kiosks suggest that their originators have confidence in the service that the kiosks provide. Kiosks have come out of the shadows. Instead of being relegated to a quiet corner, so that the user can focus on their task, kiosks are now proudly located in entrances to stores, malls and other public thoroughfares. The enhanced physical design of the kiosk makes it more difficult for users to overlook them. Kiosk housings are stylishly designed and, where appropriate, consistent with corporate images. The use of moving images either on the screen itself, in the form of video feeds or animation, or on television screens above the kiosks attracts attention. Now users notice them, approach them and use them on their way through a thoroughfare.

Customer service kiosks designed to support the activities of the 'customer in context' will be different in each context. There is an important distinction to be made between environment and context. Environment is the physical environment in which the kiosk is located, and has characteristics such as noise level, propensity to interruption, traffic and lighting; these issues are discussed, to an extent, in the ergonomics literature [Smith1997]. Context embraces environment, but also includes other dimensions of the customer experience. These include the activities and purpose of the customer when they encounter the kiosk, and even social and emotional factors. Context is concerned with the way in which the kiosk experience is integrated into, or interfaces with the wider travel, leisure or shopping experience.

3.2 Security

A complete view of the security definition employed throughout this contribution is summarized within Figure 1. The figure shows that information security has four security requirements. These requirements identify what is strived for. The security requirements can be satisfied by appropriately implementing security services. Security services can in its turn be divided in security mechanisms. With the appropriate security mechanisms the actual security requirements for information systems can be fulfilled.



3.3 General threats to Information Systems

Technological development, technical problems, extreme environmental events, adverse physical plant conditions, human institutions all present challenges to the smooth functioning of information systems. Threats to information systems may arise from intentional or unintentional acts and may come from internal or external sources. They range from cataclysmic events to minor, daily inefficiencies. Down-times, for example, may be caused by large break-down or frequent slow-ups or service degradations. The frequency and duration of disturbances, however minor, should be considered when planning for security. Large and small events may be equally disruptive to system functioning and use and equally debilitating to the organization's effective operation.

Technical factors leading to failures of information systems are numerous, sometimes not well understood, and constantly changing. They may be computer and communications hardware or software faults and malfunctions, caused by bugs, overloads or other operational or quality problems. The difficulty may arise in an internal system component (system collection of computer system or a distributed system; application and operating system software, such as a compiler or editor; LANs), an external system component (telecommunication circuits, satellites) or from the interaction of different parts of the system.

Technical problems may be caused by intentional attacks on the system. Viruses, often introduced into the system via infected software, parasites, trap doors, Trojan horses, worms, and logic bombs are some of the technical means used to disrupt, distort or destroy normal system functions.

The difficulty of providing security for networks and information is compounded in multiple-vendor environments. For example, a significant problem is the availability of access-control software, a commonly-used security measure, which is compatible with the entire system in a multiple-vendor environment. In order to facilitate development of effective security for information systems, standards bodies, governments, and vendors and users of information systems must agree on standards for security measures.

Human beings and the institutions they establish to reflect their values, whether social, economic or political, as well as the lack of such institutions, all contribute to security problems. The diversity of system users (employees, consultants, customers, competitors or the general public) and their various levels of awareness, training and interest compound the potential difficulties of providing security.

Lack of training and follow-up about security and its importance perpetuate ignorance about proper use of information systems. Without proper training, operators and users may not be aware of the potential for harm from system misuse. Poor security practice abound. Operators and users may not take even the most rudimentary security measures.

A variety of means is available for identifying a person, in order to associate data with them. These include:

- appearance - or how the person looks;
- social behaviour - or how the person interacts with others;
- names - or what the person is called by other people;
- codes - or what the person is called by an organisation;
- knowledge - or what the person knows;
- tokens - or what the person has;
- bio-dynamics - or what the person does;
- natural physiography - or what the person is; and
- imposed physical characteristics - or what the person is now.

If we omit now the first four identification marks the fifth is knowledge i.e. what the person knows. Mostly under this term is a password.

The choice of a password, a nearly universal user activity and usually a user's first activity on a system, provides a striking example. Although passwords are employed to control access to most information system, few users are instructed on the need for password

security, on the manner in which to create a password or on penalties for misuse of the system. Without guidance, many users choose obvious passwords that may be easily ascertained, such as family or pet names, joke words or words related to the task. After logging in to the system, untrained users may leave active terminals connected to network systems unattended, display passwords on the side of terminals, fail to create backup data files, share user identification codes and passwords, and leave open access-control doors into high security areas. These are threshold security problems that arise form entering a room, switching on a computer or terminal, possessing a password and logging in.

Tokens - or what the person has is for example smart cards, flash memory etc., so some things which is able to communicate through computer or other equipment with information system with only one aim to help information system recognize access person.

Bio-dynamics - or what the person does is now very frequently in use. For example, human being behaviour likes way of talking, way of moving, way of writing, etc.

Natural physiographic - or what the person is; and imposed physical characteristics - or what the person is now meaning for example, eyes, hands, fingerprint, etc, etc.

Errors and omissions may occur in gathering, creating, processing, storing, transmitting, and deleting data and information. Failure to back up critical files and software multiplies the negative effects of errors and omissions. If files have no been baked up, the organization may incur significant expense in time and money in recreating them.

Intentional misuse of authorized system access and unauthorized system access ("hacking") for the purposes of mischief, vandalism, sabotage, fraud or theft are additional serious threats to system and organizational viability. Unauthorized copying of software (software piracy), for example, is widespread. Popular conception holds that the greater part of threats to information systems comes from external sources. On the contrary, persons who have been granted authorized access to the system may pose a larger threat to information systems. They may be honest, well-intentioned employees who, owing to fatigue, inadequate training or negligence, commit an inadvertent act that deletes massive amounts of data. They may be disgruntled or dishonest employees who misuse or exceed authorized access to tamper deliberately with the system for their own enrichment or to the detriment of the organization.

Computer programs are an important element of information systems and a potentially fertile terrain for threats to information systems. A program containing a virus that is introduced into an information system may affect the availability, confidentiality and integrity of that system by overloading the system, changing the list of authorized users of certain parts of the system or altering data or information in the system. Violations of provisions of licensing agreements relating to the information system (e.g., software licensing agreements, database licensing agreements) may pose an additional security threat. Unauthorized alteration of the licensed program, for example, may trigger malfunctions as the modified software interacts with other parts of the system. Disclosure of proprietary information may damage an organization's competitive position.

Insufficient use of systems may also lead to security problems, such as maintaining information availability or integrity in the event of shortages of qualified personnel, whether

as a result of employees changing jobs, the introduction of new technologies requiring new skill, or work slowdowns, stoppages or strikes.

Social, political and economic institutions have not kept pace with technological development and growth in use of information systems. The price is uncertainty and lack of uniformity, which increase expense, cause delays and, if permitted to continue, might impede future growth. There is a glaring deficiency of codes of practice, standards, and legal guidance and apportionment of legal rights and obligations.

3.4 Security Failures

Security failures may result in direct and consequential losses. Direct losses are those to: the hardware, including processors, workstations, printers, disks and tapes and communication equipment; software, including systems and applications software for central and remote devices; documentation, including specifications, user manuals and operation procedures; personnel, including operators, users, and managerial, technical and support staff; and physical environment, including computer rooms, communications rooms, air conditioning and power supply equipment. Although direct losses may account for a small percentage of total losses arising from a security failure, nonetheless, the absolute investment in developing and operating the system will usually have been significant. The system requires protection in its own right as the container and channel for the data and information. The need to protect the system and the manner of doing so are inextricably linked to protecting the data and information that the system stores, processes and transmits in order both to preserve the availability, confidentiality and integrity of the data and information and to prevent alteration or damage of the container and channel through introduction of data and information, such as viruses, that may have a deleterious effect on operation and use of the system. A consequential loss may occur when an information system fails to perform as intended. Consequential losses resulting from security failures may include: loss of goods, other tangible assets, funds or intellectual property; loss of valuable information; loss of competitive advantage; reduction in cash flow; loss of orders business; loss of production efficiency, effectiveness or safety; loss of customer or supplier goodwill; penalties from violation of statutory obligations; and public embarrassment and loss of business credibility. Consequential losses account for most of the losses arising from security lapses. In light of the fact, protection against consequential loss, which, above all, means protecting the data and information, must be a top priority.

4. Conclusion

The contribution shows that the introduction of the e-government into the every day life is still far from the users. The problems connected with making the e-government into the praxis is solved step by step according the needs of countries. It is supposed the at the first will be fully work e-government within the high developed regions which means not only high developed from material point of view, but also from spiritual point of view or better speaking educational point of view. Last but not least is group of problems connected with safety accessing to the information systems here presented as a portals. The use of information systems to collect, store and cross-reference personal data has increased the need to protect such systems from unauthorized access and use. Methods to protect information systems include user verification or authentication, file access control, terminal controls and network monitoring. Such measures generally contribute both to the security of information systems and to the protection of personal data and privacy. It is possible that certain measures adopted for the security of information systems might be misused so as to violate the privacy of individuals. Information systems may include hardware, computer programs, databases, layout designs for semiconductor chips, data and information, elements of which may be protected by intellectual and industrial property laws. Intellectual property in information systems is intangible,

may cross borders virtually imperceptibly, and may be vulnerable to theft by the effort of one finger in a matter of seconds without taking the original and without leaving a trace. Security of information systems may reinforce the protection of intellectual property by limiting unauthorized access to components of the system, such as software or competitive information.

All jurisdictions offering e-government need to implement security measures to protect against external and internal threats, and higher risk sites will require greater security than others. Local governments should assess risks to their Web sites and related equipment and databases. Based on that assessment, they should develop security policies to protect their investments. Local governments should install "firewalls," use up-to-date antivirus programs and be prepared for security incidents. They should manage employee access to the Web site and related data. Local governments should test security measures and provide for outside parties to assess whether security is sound.

5. Bibliography

[And2001] Anderson R.: Security Engineering. John Willey 2001 ISBN 0-471-38922-6

[Hauer at all. 2002] Jody Hauer (project manager), Jan Sandberg, Kathryn Olson, Carrie Meyerhoff, and Leah Goldstein Moses. *A Best Practies Review Local E-Gov ernment* (Minetosa 2002 http://www.auditor.leg.state.mn.us/ped/2002/pe0208.htm)

[Stall2003] Stallings W.: Cryptography and Network Security: Principles and Practice. Prentice Hall 2003, ISBN: 0-13-091429-0

[Stall2005] Stallings W.:Business Data Communications. Prentice Hall 2005 ISBN: 0-13-144257-0

[Row1995] J. Rowley. *Multimedia kiosks in retailing*. (International Journal of Retail & Distribution Management,1995 23(5), pp.32–40.)
[Smith1997] A.Smith, *Human-computer factors.* (New York: McGraw-Hill. 1997)

[Slack at all. 2002] F. Slack, J. Rowley, *Kiosks 21: a new role for information kiosks?* (International Journal of Information Management 22 (2002) 67–83)

www.**ukonline**.gov.uk

Autors:

prof. Ing. Jan Čapek CSc.
Faculty of Economics and Administration
University of Pardubice

Studentská 95, 53210 Pardubice

Czech Republic
e-mail: capek@upce.cz
voice: +420 466 036 512

Assoc. prof. Ing. Iva Ritschelova, CSc.
Faculty of Environmental Studies
Jan Evangelista Purkyne University in Ústí nad Labem
Králova Výšina 3132/7, 40096 Ústí nad Labem
Czech Republic
e-mail: ritschelova@rek.ujep.cz
voice: +420 475 282 210