Preface


The international conference cycle EGOVIS focuses on information systems and ICT aspects of e-government. Information systems are a core enabler for e-government/governance in all its dimensions: e-administration, e-democracy, e-participation, and e-voting. EGOVIS 2016 brought together experts from academia, public administrations, and industry to discuss e-government and e-democracy from different perspectives and disciplines, i.e., technology, policy and/or governance, and public administration.

The Program Committee accepted 22 papers from recent research fields such as open data and government cloud, identity management and e-government architectures, innovation, open government, intelligent systems, and semantic technologies applications. Beyond theoretical contributions, papers cover e-government experiences from all over the world; cases are presented from Europe and South America.

These proceedings are organized into eight sections according to the conference sessions.

We were honored that the keynote speeches, hosted this year by EGOVIS, were given by three leaders in the e-government field from academia and the public sector: Prof. Ronald Traunmuller of the University of Linz, one of the pioneers in e-government studies, discussed the information system perspective in e-government research and development. Attila Péterfalvi, President of the National Authority for Data Protection and Freedom of Information in Hungary, gave an overview of the transparency of public functions and public funds in Hungary. Finally, Prof. András Gábor from Corvinus University in Budapest addressed the problem of security governance, in particular for public sector services with regard to the social components of trust.

The chairs of the Program Committee wish to thank all the reviewers for their valuable work; the reviews raised several research questions that were discussed at the conference. We would like to thank Gabriela Wagner for the administrative support and assisting us in the scheduling.

We wish our readers a pleasant and beneficial learning experience and we hope that the discussion between researchers will continue after the conference contributing to building a global community in the field of e-government.

September 2016
Enrico Francesconi
Andrea Kő
Organization

General Chair
Roland Traunmüller University of Linz, Austria

Program Committee Co-chairs
Enrico Francesconi Italian National Research Council, Italy
Andrea Kö Corvinus University Budapest, Hungary

Honorary Chairs
Wichian Chutimaskul King Mongkut’s University of Technology, Thailand
Fernando Galindo University of Zaragoza, Spain

Program Committee
Luis Álvarez Sabucedo Universidade de Vigo, Spain
Jaro Berce University of Ljubljana, Slovenia
Francesco Buccafurri Università degli Studi Mediterranea di Reggio Calabria, Italy
Alejandra Cechich Universidad Nacional del Comahue, Argentina
Wojciech Cellary Poznan University of Economics, Poland
Wichian Chutimaskul King Mongkut’s University of Technology, Thailand
Flavio Corradini University of Camerino, Italy
Vytautas Cyras Vilnius University, Lithuania
Joan Francesc Fondevilla Gascón Universitat Pompeu Fabra, Spain
Enrico Francesconi Italian National Research Council, Italy
Ivan Futo National Tax and Customs Administration, Hungary
András Gábor Corvinus University of Budapest, Hungary
Fernando Galindo University of Zaragoza, Spain
Francisco Javier García Marco University of Zaragoza, Spain
Stefanos Gritzalis University of the Aegean, Greece
Henning Sten Hansen Aalborg University, Denmark
Christos Kallioutis University of the Aegean, Greece
Nikos Karacapilidis University of Patras, Greece
Evangelia Kavakli University of the Aegean, Greece
Bozidar Klicek University of Zagreb, Croatia
Ah Lian Kor Leeds Beckett University, UK
Hun-yeong Kwon | Korea University, South Korea
Andrea Kő | Corvinus University Budapest, Hungary
Christine Leitner | Centre for Economics and Public Administration Ltd. (CEPA), UK
Herbert Leitold | E-Government Innovation Center EGIZ, Austria
Marian Mach | Technical University of Kosice, Slovakia
Peter Mambrey | University of Duisburg-Essen, Germany
Mara Nikolaidou | Harokopio University of Athens, Greece
Javier Nogueras | University of Zaragoza, Spain
Monica Palmirani | University of Bologna, Italy
Aljosa Pasic | Atos, Spain
Andrea Polini | UNICAM, Italy
Reinhard Posch | Technical University of Graz, Austria
Aires J. Rover | Federal University of Santa Catarina, Brazil
Christian Rupp | Federal Chancellery of Austria/Federal Platform Digital Austria, Austria
Erich Schweighofer | University of Vienna, Austria
Hatem Ben Sta | National University of Ireland Galway, Ireland
Ella Taylor-Smith | Edinburgh Napier University, UK
Raisa Uskenbaeva | International University, Kazakhstan
Julian Valero | iDertec, University of Murcia, Spain
Costas Vassilakis | University of the Peloponnese, Greece
Gianluigi Viscusi | EPFL - CDM -CSI, Switzerland
Christopher C. Wills | Caris Research Ltd., UK
Frank Wilson | Interaction Design, UK
Robert Woitsch | BOC Asset Management, Austria
Chien-Chih Yu | National ChengChi University, China (Taiwan)

Additional Reviewers

Stavros Simou | University of the Aegean, Greece
Evangelos Gongolidis | University of the Aegean, Greece
Nikos Argyropoulos | University of Brighton, UK
Maria Sideri | University of the Aegean, Greece
Angeliki Tsouhou | Ionion University, Greece
Prokopis Drokaris | ENISA, Greece
Agustina Buccella | GIISCo, University of Comahue, Argentina
Andrés Flores | GIISCo, University of Comahue, Argentina
Abstracts of Invited Talks
Transparency of Public Functions and Public Funds - Controversial Actions in the Field of Transparency of Public Funds in Hungary

Attila Péterfalvi
Hungarian Data Protection and Freedom of Information Authority
peterfalvi.attila@naih.hu

Abstract. As clearly stated by the Hungarian Constitutional Court: ‘without being monitored by its citizens, the state becomes an unaccountable and unpredictable machine, and this is especially dangerous because a non-transparent state represents an increased threat to constitutional rights’.

The freedom of information is one of the most sensitive rights in a democracy, because the political forces always would like to follow their own trend to communicate their vices and virtues. In opposition they urge a larger publicity, whereas as governing force they prefer to communicate according to their own perceptions.

Since the constitutional revolution of 1989, there were two governmental periods when the legislation opened more transparency on national assets: the first one was in 2003 when the left-wing coalition adopted the “Glass pocket Law”, the second one was the right-wing coalition in 2012, when by the constitutional revolution, the Fundamental Law itself decrees the transparency on national assets.

The new Hungarian Fundamental Law in its preamble – called NATIONAL COMMITMENT AND BELIEF – proclaims that “true democracy exists only where the State serves its citizens and administers their affairs justly and without abuse or bias”.

In Hungary the fundamental right of freedom of information has to react to the new/old functions of the State. The wide spread of State Owned Enterprises (SOEs) gave a new perspective of publicity of data in connection of financial data of these enterprises.

On one hand the legislation widened the FOI with the new constitution, what gives a quite strong basis of freedom of information:

- first of all, the Fundamental Law declares the right to know as a fundamental right,
- in addition, it creates the national constitutional foundations of transparency of public funds, of public property.

Till nowadays SOEs fall under the more or less the same transparency regulations as public bodies. According to the 2007 CVI Act on State Ownership, the State may acquire (or dispose of) assets in order to: (1) execute State functions; (2) fulfil societal needs; and (3) realise government economic policy goals. In practice, some rationales for state ownership that have been put forward, in addition to the “general public interest” have included energy security, delivering country-wide, affordable mail
services (the Hungarian Postal Service Co.) or fulfilling cultural facilitation functions (the Hungarian National Film Fund).

State-Owned Enterprises filled a gap in the publicity of public funds. A body or person that is vested with powers to manage or control State property shall be treated as a person or body exercising public functions pursuant to the act on access to information of public interest. According to the Hungarian legal background, with the help of the Constitutional Court’s interpretation, a body or person that is vested with powers to manage or control State property shall be treated as a person or body exercising public functions pursuant to the act on access to information of public interest.

This wide sense of public body motivated that our Authority gave recommendation on the borders of business secret and freedom of information. Our conclusion was that these state-owned business players – within strict conditions – could justify the secrecy of their management data, but they have to provide enough data to the public to control the use of the national assets.

This wide sense of transparency of public funds motivated the legislature to modify sectoral laws to “rationalize” the FOI. For example, in 2014 Hungarian lawmakers have voted to classify some data in contracts on the expansion of the Paks II nuclear power plant for 30 years. The Paks II Act classifies all data and contracts related to the planned €12.5 billion ($14 billion) expansion of the Paks II nuclear power plant by Russia, for 30 years. In March 2016 the Hungarian Parliament approved new disclosure exemptions for the state-owned postal service and for foundations established by the National Bank of Hungary. In Mai 2016 the 2017 Central Budget Act modified the Act CXXII of 2009 on the More Economical Operation of State-Owned Enterprises non-disclosure protections of data relating to the assets, functioning and contracts of state companies involved in activities such as central data acquisition and telecommunications management could be exempted from Freedom of Information (FOI) laws for up to 30 years.

Furthermore, the central and principal budgetary transparency, and the state’s (new) quasi business functions, there is a quiet significant importance of transparency of political parties’ finances. The FOI legal literature always tried to find real solution to legislature to find the way to wide transparency of parties finances.

To summarize the most overall theme of transparency of the state and fight against the corruption is the notion of public function, public funds. What are the borders of public functions and business sector, can we treat he same way the SOEs in monopoly and the traditional public bodies etc.?
The IS Perspective in E-Government Research and Development

Roland Traunmüller

Johannes Kepler Universität Linz, Altenbergerstraße 69, 4040 Linz, Austria
traunm@ifs.uni-linz.ac.at

Abstract. Five years ago DEXA established a Conference line under the name of EGOVIS as to underscore the importance of the Information Systems view. Obviously, the Information Systems aspect plays a pivotal role in the whole field of E-Government Research and Development. The term denotes the study of organizational systems with a specific reference to information and the complementary networks of hardware and software. It comprises a quite broad scope and thus addresses a breath of themes ranging from a strategic and design focus to managerial and operational questions. Accordingly, the IS Perspective induces a holistic and comprehensive approach for E-Government R&D. In addition it helps to comprehend and improve a series of actual and novel innovations. The contribution outlines first the general merits of the IS perspective and consequently moves to discussing some recent challenges. Respective themes comprise Collaboration Features, Mobile Government, Open Government and Modelling Approaches.
Trust or Security – Stakeholders’ Responsibility

András Gábor
Corvinus University of Budapest
andras.gabor@uni-corvinus.hu

Abstract. Security is one of the most often used term in the world of ICT. It is very likely, security and in a closer look the information security is an important phenomenon. The total expenditure on information security in 2015 was estimated by Gartner to 75.4 billion USD, 4.7 % growth compared to 2014 spending.

Demand for security goes back in time well before the age of ICT, somehow in parallel with the level of vulnerability. Vulnerability is the likelihood of losing something what is in our possession, nevertheless if we worked for it, or inherited it. The likelihood of losing something depends on the variety and extent of threats. Occurring a negative event which effects individuals, organisation, physical objects, processes, etc. in a bad way often call risk. Risk management takes into account the risk with the likelihood of occurrence and how serious is the consequence of the bad event. This way the weighted risk stands in front of the security measurements. Security measurements tend from the very simple physical solutions (e.g. fences) through the logical level solutions (e.g. authentication) up to the strategic level security governance.

If we raise the question, how much money is worthwhile to send on security, in order to minimize the vulnerability (=the potential loss), the answer is easy and simple. The spending on security is justified up to the level where cost of security is still a little bit less or maximum equal to the value of the potential loss. This is the answer to the question, if… we are fully in aware of the value of every property what we have. But how can we translate the value of every property on monetary tools? Anyhow.

From the angle of threat-types, they can be grouped in several groups. In the following we focus on the information security, only. The scale starts from blocking the use of an information system, information service (Denial of Service, DOS), through spamming, alteration of data, identity thieves, money flow diverting, industrial espionage up to destroying data. As a consequence, there are effective financial losses, e.g. if an outgoing invoice file is destroyed, the company cannot claim money from its customers. Beside of financial losses, important know-how can be transferred to the competitor, which may create indirectly financial losses. On the level of individuals personal or very special personal (e.g. health status) can be stolen and misused. These and similar problems encourages the ICT managers increasing the level of security, but the calculation of the needed level is in a grey zone, since no exact information of the monetary sum of potential losses.
The problem is even more complex, because due to national security, anti-cyberterrorism, budgetary reasons (tax offices), competition law (anti-trust, anti-cartel actions), and many other community reasons there is a social need for "legal backdoors" in properly secured information systems, the state is eagerly needs the data of its enterprises and citizens. Without questioning the rationality of data inquiry of the state, it raises extra security, data privacy issues.

Back to the original question, what is the sufficient extent of security spending or effort?

The usual approach is the weighted risk analysis (risk likelihood x impact), based on the foreseeable potential loss is a reliable basis, what kind of efforts are justified in order to spend on security.

Behind of the vulnerability and threats (risk) and the security measures in most of the cases work strategies. Strategy means in this case properly defined goal or goals (to block services, to get secret or hidden information, etc.) and procedures aiming to reach the goals. On the other hand, security management has the opposite goals and the suitable procedures. Game theory addresses typically similar problems, therefore it is worthwhile to investigate whether game theory can be applied in the security domain. From game theory angle this is an equilibrium problem, especially if we take into consideration its dynamical character.

Having a deeper look into goals and strategies, we find, the goals are relatively more stable, while strategies changes frequently. The reason of variety of strategies partly explained by the fast changing technology, partly is due to the different social environment. Social engineering as a separate industry branch has developed on the ground of social components of the security. Having analysed and decomposed the social environment we found the trust as one of the most effective factor. Trust on the contrary of "hard" (=well-defined) security procedure, is a "soft" concept.

Trust by a very general definition is a set of beliefs, according to which interacting other parties are benevolent. Trust has different interpretation in psychology, in sociology, in social psychology, in economics, in philosophy. Many other concepts are linked to the concept of trust, like reliance, trustworthiness, stereotypes, values and value sharing, - the list is quite long. From security point of view, the social psychological interpretation looks the most relevant. From this approach trust is a common belief in a given community (society, or the effected part of the society) which is based on the combination of shared values and expectations. The recent Panama offshore case highlight the complexity of trust issue. The Panamian law firm Mossack Fonseca offered services for shell corporations for tax evasion, money laundry and many other illegal actions. After leaking the list of its customers, investigating journalists published several very delicate issues, pushing governments to act. From the point of view of the law firm the leakage created a big security problem (an employee was the highest risk factor, as always), however this security breach fits very well to high priority social and ethical values, and apart from the interested parties the belief of citizens in justice, order, in other words trust is strengthened. The list of positive and negative examples is endless.

Trust therefore can be reformulated also as strategy, in the sense of expectations and procedures. Expectations strongly correlates to the shared values and the variety of the priority order of values, less variety of priority orders, stronger the effect of the
values on the procedures. Procedures are very much linked to the actions which may follow the negative effect of trust (“being betrayed”, disappointment, losing confidence). In the above example, publicity which will push governments to rethink regulations.

At this point there are different situations, different players, and different strategies, both on the security and trust “side”. What is interesting at which point the prevention break-into actions (=security measures) will be in equilibrium with the actions-to-do (strategies) based on social-economic-individual requirements (=trust)? We believe the security and trust phenomenon can be approached, investigated through seeking the equilibrium among them.

Plenty of research issues arise, just to mention one which equilibrium concept fit better: Nash equilibrium or Pareto? How to operationalize strategies behind of trust? What can be taken into account as payoff? How to cope with the global character of the virtual world and the geographically diverse communities, hence trust (components, level) geographically, sociologically diverse nature?

Despite of the plenty open questions, one conclusion already can be drawn: the good security governance should address not only the advanced technical, technological solutions but should be open to the trust issues, security strategy must be based also on the socio-components of the trust.
# Contents

## E-Government Cases - Legal Issues

Estonian e-Residency: Benefits, Risk and Lessons Learned. .......................... 3  
*Taavi Kotka, Carlos Ivan Vargas Alvarez del Castillo, and Kaspar Korjus*

Proposal for Implementing the EU PSI Directive in Serbia. .......................... 16  
*Valentina Janev, Vuk Mijović, and Sanja Vraneš*

## E-Government Cases - Technical Issues

The Design of the Estonian Governmental Document Exchange Classification Framework .................................................. 33  
*Dirk Draheim, Kaarel Koosapoeg, Mihkel Lauk, Ingrid Pappel, Ingmar Pappel, and Jaak Tepandi*

How to Build Trust-Aware Voting Advice Applications? .............................. 48  
*Aigul Kaskina and Nevena Radovanovic*

E-Government Services Migration to the Public Cloud: Experiments and Technical Findings ........................................... 62  
*Taavi Kotka, Bruce Johnson, Tomaz Cebul, Luka Lovosevic, and Innar Liiv*

## Open Data and Transparency

Linked Open Data and e-Participation in the EU Law-Making Process .............. 79  
*P. Schmitz, E. Francesconi, B. Batouche, B. Dombrovski, D. Duy, S.P. Landercy, and V. Parisse*

A Strategy to Gradual Implementation of Data Interoperability ..................... 90  
*João Baptista Gonçalves and Luisa Domingues*

Italian Open and Big Data Strategy ............................................................ 105  
*Fernanda Faini and Monica Palmirani*

## Knowledge Representation and Modeling in E-Government

Using a Citizen Language in Public Process Models: The Case Study of a Brazilian University ................................................... 123  
*Luiz Paulo Carvalho, Flávia Santoro, and Claudia Cappelli*
Application of Legal Ontologies Based Approaches for Procedural Side of Public Administration: A Case Study in Hungary

Bálint Molnár, András Béleczki, and András Benczúr

Modeling Relevant Legal Information for Consumer Disputes.

Cristiana Santos, Víctor Rodriguez-Doncel, Pompeu Casanovas, and Leon van der Torre

Intelligent Systems in E-Government

Design of Public Sector Websites: Findings from an Eye Tracking Study Emphasizing Visual Attention and Usability Metrics

Hanne Sørum

Research Challenges of ICT for Governance and Policy Modelling Domain – A Text Mining-Based Approach

Andrea Kő and Saira Gillani

Semantic Application for the Internationalization Audit of Higher Education Institutions

Katalin Ternai and Ildikó Szabó

Using Collaborative Filtering Algorithms for Predicting Student Performance

Juan Manuel Adán-Coello and Carlos Miguel Tobar

E-Government Research and Intelligent Systems

Integrated Quality Assessment of Linked Thesauri for the Environment

Riccardo Albertoni, Monica De Martino, and Alfonso Quarati

Identifying the Main Problems in IT Auditing: A Comparison Between Unsupervised and Supervised Learning

Patrícia Maia, Leonardo Sales, and Rommel N. Carvalho

E-Government Cases - Data and Knowledge Management

Effective Biosecurity Knowledge Management: A Provenance Perspective

Qing Liu, Yanfeng Shu, and Chris Peters

A Method of Inspecting and Applying Open Government Data in the Auditing Courts of Brazilian States

Walter Gonçalino da Silva Cruz, Cristiano Maciel, Fernando B.M. de Castilho, and Natalina Namie Hirata Girata
Electronic Document Certification Service: An Enabler of e-Government
Uptake in Hungary ................................................................. 276
Péter József Kiss, József Károly Kiss, and Gábor Klimkó

Identity Management in E-Government

Implementing Advanced Electronic Signature by Public Digital Identity System (SPID) ................................................................. 289
Francesco Buccafurri, Lidia Fotia, and Gianluca Lax

Digital Signatures Workflows in Alfresco. .................................................. 304
Patrícia R. Sousa, Pedro Faria, Manuel E. Correia, João S. Resende, and Luís Antunes

Author Index .................................................................................. 319