Paper

# Innovative approach to identity management solution development for e-government at EU level

Kamelia Stefanova, Dorina Kabakchieva, and Lia Borthwick

**Abstract— This paper presents the main aspects of research, analysis and design of the open identity management architecture for e-government development within GUIDE, a project financed by the 6FP of the EC. The most important identity management issues strongly influencing the European e-government development are briefly discussed. An emphasis is placed on the innovative interdisciplinary approach used in GUIDE, aimed at covering the whole range of technical, process, policy, legal and social identity management issues, and seeking to overcome the existing fragmentation of identity management initiatives. GUIDE brings together the European industrial, financial and technical market leaders in e-government solutions, as well as leading academic institutes of the relevant scientific disciplines. Through its scientific, technological and socio-economic goals GUIDE will contribute towards initiatives that will ultimately deliver multiple benefits to governments, citizens and businesses.**

***Keywords— identity management, open identity management architecture, e-government, interoperability.***

## 1. Introduction

In March 2000, European heads of state and government meeting in Lisbon set the objective to make the European Union the most dynamic and competitive knowledge-based economy in the world by 2010, capable of sustainable economic growth with more and better jobs and greater social cohesion, and respect for the environment [1]. The e-government is one of the key areas of the EU's information society policy where further progress is required to reach the objectives of the Lisbon strategy. There is indeed a growing consensus that e-government is now becoming a key factor for increasing competitiveness. Better quality public services, more responsive and fit to their users' needs, provided electronically by more efficient public administrations, are perceived as essential to reap the benefits of the information society and reach the objectives of the Lisbon strategy.

For leaders in the public sector, the emerging debate over identity management and the selections of technology to authenticate citizens and business are among the most important of all matters to shape the information age advanced frames. The competing policy interests range from protecting citizen freedoms, privacy and other prerogatives on one end of the scale to ensuring law, order, national security and institutional efficiencies, on the other end.

Electronic identity management for e-government requires combination of technological, social, economic and application-oriented research, including security and privacy of the identity data; public trust and acceptability; technological, organizational and linguistic interoperability. The e-government at EU level needs a coherent approach for interrelations and compatible solutions.

This paper presents the main aspects of research, analysis and design of the open identity management architecture for e-government development within GUIDE[1]. The innovative approach towards the identity management issues within the e-government on a pan-European level, achieved as a result of the collaborative project partners' efforts, is briefly described.

## 2. Background

### *2.1. The identity management concept*

Governments have always been concerned with identity and are now confronted by the unique challenge of provisioning identity in networked world. Managing identity is a fundamental piece of what a government does, and governments are vitally concerned with identity on a daily basis. Many of the lifecycle activities involved in creating, using, changing and ending an identity rest with governments. Electronic authentication and managing digital identities is certainly different in the government setting. Relationships between government, citizens and businesses are unique and may last a lifetime. Most importantly, individuals and organizations have higher expectations for government when it comes to protecting the privacy of information. There exists a tension between citizen and business demand for efficient and accountable e-government services and expectations for privacy protection.

Identity as a crucial security feature for e-government, can be considered as a uniquely defined and maintained set of data that refers to a person (natural or legal) and used for uniquely identifying the person for particular e-government processes. In other words, Identity depends on the range of government services in Europe. Identity management should support these processes in cross-application and cross border environments.

Going deeper in the concept of identity, we discover it is broad and complex. It is defined as the quality or condition of being the same, i.e., identity is what makes entities

[1] See, http://www.guide-project.org

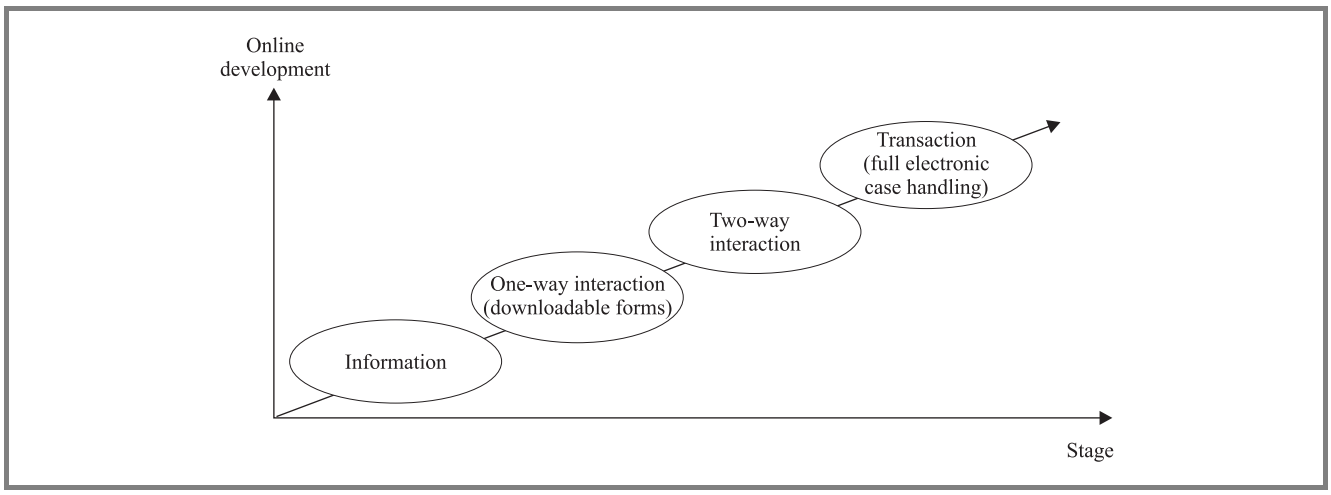



***Fig. 1.*** Progress of online services for businesses and citizens.

the same today as they were yesterday [2]. Importantly, organizations and people can have different identities when working with different systems, or can have different identities when working with a single system, perhaps when working in different roles. While names and naming protocols are a critical element of identity, in that they give us the means to call out one identified entity from another, the underlying relevance, role, context and meaning attributed to a given named individual or company can only be gleaned by reference to other factors. The full measure of identity is a subtle and multi-faceted complexity because people and organizations exist in many social, economic, political, cultural and other dimensions all at once.

It is well understood that deploying an identity management solution has many dimensions and uncertainties. Nevertheless, governments are now faced with a complex set of challenges as they are asked to balance the need for security, privacy, citizen and business demands for online services, and the issuance of digital identities to make these services a reality. This is not a simple undertaking and must be supported by a complex framework of laws, policies, institutional decisions, business practices and ultimately, technology.

As articulated in the 2002 NECCC *Identity Management White Paper* [3], the vision of identity management for e-government solutions is to "support common identity needs of governmental and private transactions" and "reduce costs of government and enhance service quality". It is well understood that this vision must be achieved under an obligation to "preserve or improve individual privacy, name and identity related liberties and the security of identity information".

The issues involved in creating, using, changing and ending an identity involve technical, procedural, legal and policy dimensions. The advent of the information age has raised many of these issues anew. Current information management capabilities provide tremendous leverage in accessing, processing, manipulating and stealing information. This raises questions of privacy, security and fair information practices on the one hand, to be balanced against convenience of e-government service delivery, the need to identify and apprehend terrorists and fraud artists, and the need to interoperate across government and private systems on the other hand.

Every EU citizen and every EU company owns rights and obligations. Many of them would expect to be able to fulfill those rights and obligations wherever they are registered or work in the EU. Access to public services at pan-European level is a key aspect of this approach. Many research efforts in the last few years are devoted to the development of a mechanism for accessing those rights and meeting the obligations, which should be straightforward, easily understandable and accessible anywhere anytime within the member states.

Increased expectations of citizens and businesses, wanting to transact with their government through the interface of their choice, and the necessity of governmental entities to interact more effectively and efficiently with each other, have led to focusing for solution development on the capabilities available through the Internet.

### *2.2. Current state of the e-government in Europe*

The improved delivery of public services is getting a very critical element of the wider economic strategy to modernize the EU economy. The European Commission's fifth annual survey of online government services in Europe [4], points out the impressive progress in developing and delivering public services online across the EU. The study reveals that over 90% of the public service providers now have an online presence, and 40% of basic public services are fully interactive. The service delivery gap between new member states and the pre-enlargement EU 15 is lower than many expected and could close very quickly. The availability and interactivity measures used in the survey show that EU's new member states have reached the level of the EU 15 from just two years ago.

The study goes further, analyzing the sophistication of the online public services provision, presented in Fig. 1, for

the target user groups, citizens and businesses. The results reveal that the services for businesses reach an overall score of 77% for online sophistication and 58% are fully available online, while the services for citizens stay at the level of 57% for online sophistication and only 27% are fully available online. One of the main reasons for this significant difference is the fact that e-government services towards business are frequently revenue-generating services for governments. Additionally, the business processes, information systems and technical infrastructures are typically better developed than the ones used with citizens and therefore businesses easily adopt e-government services.
By developing an open identity management architecture to underpin e-government solutions, GUIDE will enable governments to offer higher quality services to businesses and citizens, thus reducing administrative costs and fighting the negative consequences of the virtual space, and will also contribute to an improved collaboration between different departments and the harmonization of e-government on a pan-European level.

### *2.3. Interoperability as enabler for European e-government development*

The e-government has been developed so far in a very fragmented manner. E-government services are deployed by a multitude of public administrations at the national, regional and local level. Those services are islands of automation which cannot work together. This fragmentation may severely handicap the wide take-up and widest possible impact of e-government unless joining-up administrations and inter-linking online services is made possible through the interoperability e-government services.
According to the European interoperability framework [5], the term interoperability means "the ability of information and communication technology systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge". Three aspects of interoperability have to be considered when setting-up services designed for more than one public administration.

Organizational interoperability concerns the definition of business goals, modeling of business processes and collaboration of administrations that wish to exchange information, but that may have a different internal organization and structure for their operations. The requirements of the users should also be addressed by making services available, findable, accessible and user-oriented. Semantic interoperability includes ensuring that the precise meaning of exchanged information is understandable by any other application not initially developed for this purpose and enabling systems to combine received information with other information resources and to process it in a meaningful manner. Technical interoperability concerns linking up computer systems and services, which includes key aspects such as open interfaces, interconnection services, data integration and middleware, data presentation and exchange, accessibility and security services.

One of the main objectives of GUIDE is to establish the EU as the global leader of e-government services through the enablement of an open architecture for identity management based on durable trans-national co-operation and consensus on a pan-European basis. It will be achieved by providing an architectural vision that integrates local, national, and international (pan-European) identity management services to establish a conceptual identity management grid, described below.

## 3. GUIDE open identity management architecture

### *3.1. State-of-the-art in the field of e-government and identity management*

The research work carried out in GUIDE reveals that the different approaches to establishing e-government frameworks repeat some of the experiences of the enterprise domain, especially in that earlier versions focus on technical issues alone and later editions increasingly broaden the scope to organizational and policy issues. Early versions of e-government frameworks focused entirely on technical aspects, defining protocols and interfaces between systems. Over time and after several failures of architecture efforts the need for business driven approaches was widely accepted. This led to the development of layered frameworks deriving technical requirements from a pre-defined business strategy. Similarly the level of integration increases from rather low integration in early architectures to higher levels of integration in later editions.
Numerous solutions for e-government applications have evolved, each with their associated strengths and weaknesses. Most have focused only on offering a technical architecture, which neglects the incorporation of other aspects of identity management such as trusted third parties issuing and managing credentials, privacy, access control, risk and liability management. However, identity management is not just a technical issue. Identity management and perceived security are as much dependent on the context in which they are applied as on the architecture used. Moreover, every identity management solution to be implemented in the area of e-government faces the challenge to integrate smoothly with existing systems. The integration can be achieved through interoperability that can only be secured through the development of an open architecture.

Recent years have brought increasing research in the field of e-government and identity management. There are a growing number of projects in this research area, financially supported by the European Commission and uniting the efforts of leading European industrial and academic partners, e.g., the projects EMAYOR, HOPS, GUIDE.
GUIDE's mission is to lay the foundations of a generally accepted open identity management architecture for e-government on a European level. The research of GUIDE is focused on addressing the full range of technical, process, policy, legal and social issues that will allow this vision to

proceed. GUIDE brings together the European industrial, financial and technical market leaders in e-government solutions, as well as leading academic institutes of the relevant scientific disciplines.

### *3.2. GUIDE architecture framework*

Frameworks for e-government are in an early state of evolution. In this situation a look at the available solutions in the well developed enterprise domain allows adopting existing results and experiences in their development process. This is a disciplined approach to understand how components of an enterprise communicate, change, and function together as a whole [6].

An architecture is defined as a collection of independently useful systems that have been integrated together to achieve additional properties not associated necessarily with any of the individual systems. The strong focus is on communication and cooperation, and therefore the idea of interoperability between systems is paramount.

In the course of the development of the field, architectures have become more encompassing in that they do not only cover computer hardware and software, but increasingly as well organizational and business dimensions. They have as well become more sophisticated in their internal structure to respond to more demanding requirements especially for integration and flexibility.

GUIDE has assessed a number of industry approaches for architecture development such as Zachman and TOGAF8, which are implemented using Popkin system architect and RUP SE tools. At this stage of the project the Zachman model is adopted as a general framework for developing a methodology, specific to the requirements of an open identity management architecture, as it provides a starting point and an industry standard approach. However, GUIDE's research is not confined to that model. During the research and development process other approaches will also be used if considered useful and effective.

The Zachman enterprise architecture framework [7] is shown in Fig. 2. Each cell represents the intersection of a particular focus and a perspective. Each focus (the question what, how, where, who, when, and why) is depicted in a column and each perspective (point of view) – in a row. The perspectives define the point of view or the level of abstraction for the information contained in the cells. The information and models within a single row represent a complete description of the architecture from that perspective. Each column captures all of the architecture knowledge for the particular question being asked, the focus. The total architecture knowledge for each focus is obtained by isolating each focus and defining the artefacts for each perspective within it.

| | DATA *What* | FUNCTION *How* | NETWORK *Where* | PEOPLE *Who* | TIME *When* | MOTIVATION *Why* | |
|---|---|---|---|---|---|---|---|
| Objective/ Scope *Contextual* Role: Planner | List of Things Important in the Business | List of Core Business Processes | List of Business Locations | List of Important Organizations | List of Events | List of Business Goals/Strategies | Objective/ Scope *Contextual* Role: Planner |
| Enterprise Model *Conceptual* Role: Owner | Conceptual Data/ Object Model | Business Process Model | Business Logistics System | Work Flow Model | Master Schedule | Business Plan | Enterprise Model *Conceptual* Role: Owner |
| System Model *Logical* Role: Designer | Logical Data Model | System Architecture Model | Distributed Systems Architecture | Human Interface Architecture | Processing Structure | Business Rule Model | System Model *Logical* Role: Designer |
| Technology Model *Physical* Role: Builder | Physical Data/ Class Model | Technology Design Model | Technology Architecture | Presentation Architecture | Control Structure | Rule Design | Technology Model *Physical* Role: Builder |
| Detailed Representations *Out of Context* Role: Programmer | Data Definitions | Program | Network Architecture | Security Architecture | Timing Definition | Rule Specification | Detailed Representations *Out of Context* Role: Programmer |
| Functioning Enterprise Role: User | Usable Data | Working Function | Usable Network | Functioning Organization | Implemented Schedule | Working Strategy | Functioning Enterprise Role: User |

***Fig. 2.*** The Zachman enterprize architecture framework (*copyright: John A. Zachman, Zachman International*).

Service oriented architectures (SOAs) are state of the art in enterprise architectures. Conceptually, SOA represent a model of loosely-coupled applications working together by exposing services to each other. Business wise, services are expressing data- and function-services that one party can offer other parties to use. Technologically, SOA consists of a group of emerging standards that defines protocols and creates a loosely-coupled framework for programmed communication between different systems. Web services are a specific implementation of a SOA, i.e., a method which enables an application to be invoked by other applications by receiving and sending data in standardized XML.

Taking into consideration the above mentioned, the essence of the GUIDE architecture is foreseen as a service oriented architecture, given the obvious requirements for "loosely-coupled" systems, independence of implementation and location, etc. Furthermore, the only real candidate implementation of SOA currently is the web services model, and this is envisaged as the most likely physical perspective candidate for the GUIDE architecture. Given that there will be a need for a highly secure approach, it is envisaged that the service oriented security model (SOSA) as currently delivered by the emerging web services security model (WSSM), will be overlaid onto the basic WS architecture.

The design and development of the GUIDE open identity management architecture is driven by eight key political and functional axioms, to which further research is designed to add more knowledge and insight. These axioms are as follows:

1. European open identity architecture: "A European open identity architecture will be defined".
2. External applications: "All identity data is produced and consumed through applications outside the identity grid".
3. External data: "A significant amount of identity data will always stay outside the identity grid".
4. External transactions: "A significant amount of identity transactions will always be done outside the identity grid".
5. Data ownership: "Each functional element of identity data within the identity grid will have clear data ownership and data obligations".
6. Identity services: "Applications outside the grid will interact with a set of *attribute service providers* within the identity grid".

7. EU governance: "The architecture will conform to the overall EU regulatory and legal framework and system of governance".
8. State governance: "Each member state will have governance over attribute services operating within their boundaries, and the identity data underpinning these identity services".

As the development of the architecture progresses these will be supplemented, at a more detailed level, by a set of "architectural principles", including:

- Guide will adopt service oriented security architecture as its underlying architecture.
- Guide will align with and complement other EU information society initiatives, such as IDA.
- Guide will align with and complement emerging industry initiatives and standards in federated identity management, such as the liberty alliance.
- Guide will observe the principle of subsidiarity.
- Guide will be inclusive of all member states identity management requirements where these do not conflict with the majority position or can be provided as an optional feature.
- Guide will develop a proportional response to the overall requirement for pan-EU identity management, with the aim of providing maximum benefit for minimized effort.

GUIDE's strategic vision is to develop an architecture that integrates local, regional, national, and pan-European identity management services in an interoperable manner that allows accommodating the requirements of member states. As such the GUIDE architecture is consistent with the principle of subsidiarity. It is based on a federated information infrastructure model that respects the sovereignty of member states in identity management issues, rather than a hierarchical one.

In this relation GUIDE is conceived as providing a pan-European federation of identity federations, where the architecture of each constituent federation is deferred to the "owners" of the federations, including member state governments and commercial organizations. GUIDE focuses on how these federations should interoperate, such that in totality the whole can be conceived as an identity grid or identity network for Europe.

The GUIDE identity management grid presented in Fig. 3 is a high level visual representation of the concept for pan-European architecture, derived from the axioms defined above.

Central to the model is the identity holder. It represents the holder being in control of the identity. This is one of the key principles of GUIDE. The identity holder can be a physical person such as a citizen, but may also be a legal entity such as an organization, or automated agents such as web services. It should be noted in this graph, that the identity holder is not part of the grid. However, since the user is "in control" of the identity, it should be represented in the middle. One could view the identity holder as standing "above" the grid.

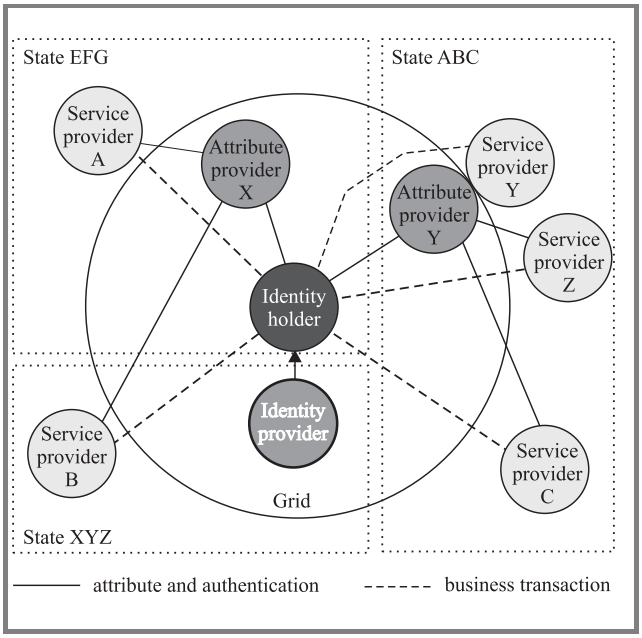



***Fig. 3.*** Identity management grid conceptual model.

The identity grid contains identity data elements. They are released under a specific set of circumstances, governed by a number of protocols. The grid is represented by the large circle and all elements that lie within it. The identity grid will be a set of physical services and data elements, controlled by procedures and policies (Axiom 1).

The service providers and their applications sit outside the grid. Service provider applications connect into the grid in order to request and process identity data elements (Axiom 2). In addition to e-government applications, commercial applications may ultimately also be allowed to utilize the grid, obviously when satisfying the GUIDE principles.

Some identity data elements will remain outside the grid for a certain period (Axiom 3). Processing of this data will be governed by protocols derived from principles on data protection, security, retention and so on. Data elements exist in databases alongside each application. Furthermore, many (non-e-government) applications and databases are outside this visual model.

The model focuses on e-government applications and their use of identity data. Hence a number of identity transactions (such as commercial transactions, and e-government service providers that are not connected to the grid) will remain outside the grid (Axiom 4).

One of the most critical activities in identity management projects is the establishment of protocols on processing of data elements. This is essential for ensuring of accuracy and quality of data, as well as for meeting other social,

legal and regulatory requirements. Data subjects will always be in control of their data – the citizens can declare how their data may be used and its accuracy maintained in certain cases. In addition, there will be legal entities that are accountable for legitimate data management (Axiom 5).

There will be a set of identity services within the grid (Axiom 6), in the form of identity service providers. Each identity service provider will be governed by an individual state and "certify" the identity of the identity holder. There may be multiple identity service providers, just as there are multiple unique IDs in various countries. In essence, each country of the EU represents a single identity service provider. Furthermore, the arrows represent the conceptual flow of data to and from identity services within the grid. Key to GUIDE is that identity service providers do not interact with service providers – an attribute service provider is set up as a mediator – with the purpose to keep the identity holder in control as much as possible.

Attribute service providers deliver the required identity attributes credentials and authentication services to the application service providers. This will depend on the strength of authentication that is required for a specific application. There may be more attribute service providers that an identity holder is affiliated with, and a service provider and attribute service provider may originate from the same entity (service and attribute service provider Y in Fig. 3).

Within the identity grid itself, the overall governance of the grid will be driven by regulatory bodies that follow rules derived from EU legislation (Axiom 7). Within the overall EU governance, individual states will carry governance over the identity data and services within their boundaries (Axiom 8). The pan-European aspect of different states is represented in the model by the dotted boxes.

### *3.3. Innovative interdisciplinary approach to identity management for European e-government development*

The formation of identity in all its dimensions is conditioned by the institutional, policy, legal, and regulatory frameworks in (or against) which it evolves. Information and communication technology broadens the scope of interaction of these frameworks, which means that institutional, political and legal frameworks that function as the drivers and sources of identity interact on a global scale. In this context identity drivers diffuse across institutional environments, borrow from each other and create amalgams that correspond to common patterns of identity formation, while adapting to the specific social environments within which they operate. This is to say that the formation of identity is a process that is mediated by antecedent, yet evolving, institutional, political, legal, and regulatory forms. This mediation is of fundamental importance in the emergence, or lack thereof, of factors that encourage the uptake of e-government services. A critical question then concerns analysis of the evolving topology of the institutional, political, legal, and regulatory sources of identity formation. Such a question can only be answered by approaches that remain sensitive to the dialectics of integration and reproduction of difference that mark contemporary EU history.

Much of the research work within GUIDE focuses on institutional, policy, legal and sociological frameworks underpinning identity management in order to identify conditions for, and obstacles to, EU-wide take-up of e-government services [8]. Central to the research is an understanding of critical organizational and political aspects of identity management. An analysis of the legislative landscape at both, national and EU level, is also undertaken, as it will give the "enabling legislative framework" that will shape the paths of development of the open identity management architecture of GUIDE. The socio-economic, ethical and cultural differences that drive identity formation will be studied and identified as well.

GUIDE, being an integrated project, stresses on "integration" of the conceptual and research components of the project. All documents, produced as a result of the in-depth studies of the institutional, political, legal, socio-economic and policy aspects of identity management, are continuously analyzed and requirements towards the developing open identity management architecture are being formulated. These requirements are directed to the identified architecture pillars and their aspects, including identity data (security, confidentiality, integrity, availability, privacy, intra- and inter-state identity data transactions, data holders, data users); identity management services (security, accessibility, user interface, standards, protocols, service providers, service users), identity management processes (security, standards, protocols, process providers, process users), interoperability, multilingualism, etc. Each requirement is given priority expressed in at least three basic ratings: compulsory, important and nice-to-have. The prioritization is performed by both, the industrial experts responsible for the architecture design and the academic researchers studying the settings, in which it will function. The importance of each requirement for the proper functioning of the architecture is primarily considered. The assigned priority is dynamic and might change with the progress of the GUIDE research and architecture design.

The key research findings and their implication for EU and member states will be synthesized and presented in one of the project deliverables titled *GUIDE Policy White Paper on Identity Management*.

### *3.4. The verification process*

GUIDE open identity management architecture will consist of a collection of identity management services integrated by a combination of technical and non-technical compliance criteria. The verification of this integrated architecture will be realized by performing different trial tests. A number of innovative identity management services will be developed and demonstrated in parallel with already existing identity management services, as part of an overall open identity management architecture. The identity management ser-

vices will be trialed with a variety of e-government applications to demonstrate the effective meeting of user requirements for these services, as well as across different geographic scenarios to ensure the broad capture of requirements and demonstrate full effectiveness in a wider variety of settings. GUIDE trials will not only provide important verification of and give inputs for the open identity management architecture being developed. They will also provide tangible evidence that the open architecture can be implemented and will provide a valuable reference case in discussions with governments and other interested parties.

## 4. The future of identity management in the e-government perspective

There are different points of view, often quite contradictory, concerning the principles which should guide the policy, legal, business and technical architectures for identity management systems and practices. However, it is necessary to devise innovative methods and approaches that support a balanced reflection of each of the competing interests.

The involved decision makers have to carefully consider the policy, technical, legal and business ramifications of identity management at all levels – local, national, European. The technical architectures chosen are not policy-neutral, in that they carry with them certain explicit or implied assumptions about the roles and expectations of users. In addition, the policy and legal approaches are charged with potential for missteps and controversy. However, it is clear that the basic drivers toward implementation of better identity management systems and methods will move European states and other stakeholders toward creating more, bigger and broader systems.

## 5. Conclusions

GUIDE's overall goal is to create the main critical requirements and principles for open identity management architecture development that will support EU e-government services interrelations and interoperability, based on durable trans-national co-operation and consensus on a pan-European basis. The vision to create a pan-European service-oriented architecture will allow the dynamic interoperable e-government services and applications throughout Europe, whilst preserving state subsidiarity. The innovation in GUIDE is the attempt to research and define how existing identity management services can inter-operate with new identity management services in a pan-European setting, and the adopted encompassing interdisciplinary approach to identity management, seeking to overcome the existing fragmentation of identity management initiatives.

Through achieving the scientific, technological and socio-economic goals GUIDE will contribute towards initiatives that will ultimately deliver multiple benefits to governments, citizens and business. Identity management can be applied to many different e-government services solutions by creating a consensus on European identity management architecture. Identity management services can be turned into key contributions to the further advancement of e-government throughout Europe to create the European market leadership.

## Acknowledgements

This work has been performed in the framework of the IST project GUIDE (IST-2003-507498), which is funded in part by the EC. The Authors would like to acknowledge the contributions of their colleagues from BT Limited, Siemens Schweiz AG, Visa International Service Association, Center for Technology and Innovation Management, Crealogix AG, ELCA Informatique SA, Budapest University of Economic Sciences and Public Administration, PricewaterhouseCoopers BV, Cyota, DeCon APS, Eesti-Taani Kommunikatsioon Ltd, Infonic Ltd, Modirum Oy, NetSmart SA, Tecnologia E Ingeneria De Sistemas y Servicios Avanzados De Telecomumicacion, Eidgenoessische Technische Hochschule Zuerich, The University of Surrey, European Institute of Interdisciplinary Research, Research Center of the Athens University of Economics and Business, ERASMUS Universiteit Rotterdam/Rotterdam School of Management, The Chancellor, Masters and Scholars of the University of Cambridge, Sofia University "St Kliment Ohridski" and DL Legal. The authors would like to acknowledge that they are solely responsible for this document and that it does not represent the opinion of the European Commission, and that the Commission is not responsible for any use that might be made of data appearing therein.

## References

[1] IDABC eGovernment Observatory, "The impact of e-government on competitiveness, growth and jobs", European Communities, 2005, http://europa.eu.int/idabc/egovo

[2] The Open Group, "Identity Management", a "White Paper", 2004, http://www.opengroup.org

[3] The National Electronic Commerce Coordinating Council, "Identity Management White Paper", in *NECCC Ann. Conf.*, New York, USA, 2002, http://www.ec3.org/Downloads/2002/id_management.pdf

[4] European Commission Directorate General for Information and Media, Capgemini, "Online availability of public services: how is Europe progressing?", 2004, http://europa.eu.int/information_society/soccul/egov/egov_benchmarking_2005.pdf

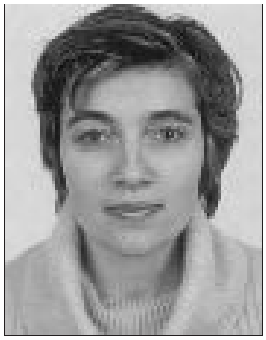
[5] IDA, "European interoperability framework for pan-European eGovernment services", Brussels, 2004, http://europa.eu.int/idabc

[6] K. Stefanova, D. Kabakchieva, and L. Borthwick, "GUIDE open identity management architecture design – key contribution to the further advancement of egovernment throughout Europe", in *5th Eur. Conf. eGovernment (ECEG 2005)*, Antwerp, Belgium, 2005, pp. 377–386.

[7] J. A. Zachman, "A framework for information systems architecture", *IBM Syst. J.*, vol. 26, no. 3, pp. 276–292, 1987.

[8] GUIDE Consortium, "GUIDE Description of Work", Ver. 4.5, Oct. 2004.

**Kamelia Stefanova** is a Project Manager at the Centre for Information Society Technologies, Sofia University. Since 1984 she has been a lecturer in information and communication technologies, teaching management information systems design. Doctor Stefanova has developed great expertise in the fields of e-government, banking and finance, knowledge economy, participating as an active researcher in many European projects.
e-mail: kamelia@fmi.uni-sofia.bg
Centre for Information Society Technologies
Sofia University
125 Tzarigradsko Shosse Blvd.
1113 Sofia, Bulgaria



**Dorina Kabakchieva** is a Project Manager at the Centre for Information Society Technologies, Sofia University. She has been actively involved in European projects within the e-government and e-business scientific areas. She has the M.Sc. degree in educational and training systems design (Twente University, the Netherlands) and the M.Sc. degree in electronics (Technical University – Sofia). Currently she is a Ph.D. student in business information systems.
e-mail: dorina@fmi.uni-sofia.bg
Centre for Information Society Technologies
Sofia University
125 Tzarigradsko Shosse Blvd.
1113 Sofia, Bulgaria

**Lia Borthwick** received the B.A. (hons) degrees in English literature and the M.Sc. in telecommunications business. She is an e-government specialist with several years experience of working in e-government and research projects. She is currently the Programme Director for Europe's largest research project on identity management for e-government. The project involves 23 organizations from industry and academia across 13 countries. She has presented at conferences in Europe, USA and India on e-government, intranets, e-business and knowledge management as well as a speech in the House of Lords to senior members of the UK government and has given a keynote speech at the World Bank's knowledge for development conference with government representatives from China, India and Brazil. Since 1997, she has had several articles published in UK trade media and has also been interviewed extensively on the issue of citizen identity management in a variety of quality and trade publications throughout Europe.
e-mail: lia.borthwick@bt.com
BT Ltd., BT Centre
81 Newgate st
EC1A 7AJ London, UK