Current Trends in Pan-European Identity Management Systems

SERGIO SÁNCHEZ GARCÍA, ANA GÓMEZ OLIVA,
EMILIA PÉREZ BELLEBONI, AND IVÁN PAU DE LA CRUZ

In a globalized digital world, it is essential that persons and entities have a recognized and unambiguous electronic identity that will allow them to communicate with each other. The demand for electronic identity has grown as a result of governments' promotion of e-Government, in which the citizen-public administration relationship often has a strictly personal nature and requires digital identification systems that are univocal, secure, and global. In particular, the European Union (EU) in 1995 launched the Interchange of Data between Administrations (IDA) program [20], as well as Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses, and Citizens (IDABC) [11], and Interoperability Solutions for European Public Administrations (ISA) [14]. These European Union programs seek to foster initiatives to achieve global interoperability between European public administrations in order to offer cross-border services.

In recent years, a number of initiatives have progressed in all member states of the EU for the introduction of electronic identities (eID) in public services and for the implementation of required management systems. In many EU countries, the electronic identification systems implemented are based on the deployment of electronic identification cards, also called eIDcards, which have begun to replace the identification cards already in customary use in some countries. The external appearance of eIDcards is similar to that of traditional ID cards, but they also include a chip that can electronically store information on the identity of the owner.

The management of this identity by public administrations is an important challenge that sharpens when interoperability among the public administrations of different countries becomes necessary. Procedures for starting a company abroad, moving home or working abroad, arranging your pension online if you retire to another country, or registering at a foreign school or university are some examples requiring interoperability. In all these cases, problems arise because persons and entities usually have different credentials depending on their own national legal framework.

In general, due to the diversity of systems employed in identity management, when a user of a system (citizen, company, or Administration) wishes to communicate with public administrations outside the scope of their local system, Identity Management Systems (IDMs) must communicate and understand each other. Different technologies, credentials, and legal frameworks cause interoperability problems that prevent correct access to public services in a cross-border scenario like the present-day European Union. Hence, the development of a single European space will require the establishment of an interoperability framework for electronic identity management systems (eIDMs), consisting of a set of technical and organizational infrastructures that can define, administer, and manage attributes related to citizens' identity.

With this aim in mind, the EU has for a number of years been pursuing several programs and action plans. Worthy of note is the *eEurope 2005 Action Plan*: *An Information Society for All* [1]. In addition, the *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All* [2], published in 2006, proclaims citizens' right to secure and comfortable access to services and establishes secure systems for mutual recognition of national electronic identities for public administration websites and services. More recently, the *eGovernment Action Plan 2011-2015* [3], published at the end of 2010, also sets out as one of its priorities the establishment of interoperable systems in both identification and authentication in the EU.

The EU has also regulated member states through a number of directives such as the IDABC [4]. Arising from this there are a number of initiatives focused on achieving interoperability between identity management systems at a pan-European level on the basis of different technologies and approaches. These initiatives seek to provide a medium-term solution to these needs while meeting the demands of European directives. Even though these initiatives have been in existence since 2004, in practice, interoperability between identity management systems of different member countries of the European Union remains more an ambition than a reality. The complete implementation of a solution, as envisioned in the *eGovernmentaction Plan of 2006* for the year 2010, is still far from being achieved.

This can be clearly seen in the presentation of the *European Digital Agenda* [5], of which the new *eGovernmentAction Plan 2011-2015* [3] is a part. With regard to key enablers for the development of eGovernment at a European level, it is established in these reports that Europe needs better administrative cooperation to develop and deploy cross-border public online services, including practical eIdentification and eAuthentication solutions. In 2012, the Commission will propose a Council and European Parliament Decision to ensure mutual recognition of eIdentification and eAuthentication across the EU, based on online "authentication services" to be offered in all member states (which may use the most appropriate official identification documents — issued by the public and private sectors). Hence, the interoperability of identity management systems is a current and

burning issue on the pan-European level for which solutions are being sought through ambitious research projects.

Evolution and Trends in Pan-European Digital Identity Systems

Our analysis of the initiatives and projects undertaken since 2004 leads to the conclusion that proposed architectures or systems, whether theoretical or practical, to achieve interoperability in identity management are based on the use of federation. As we will see, the use of this base, complemented by other technologies, provides solutions that could be more or less satisfactory.

One of the first proposals for interoperability in identity management combined federation and circles of trust. This proposal was based on the establishment of a federated network of identity management in which users, administrations, and companies in the European Union could participate in exchanges of information identity without compromising the privacy and security of information. This idea, which emerged in the project GUIDE [6], required the affiliation of all participants in circles of trust based on operational agreements that would define the trust relations between them. (See Fig. 1.) Thus, a circle of trust was a federation of service providers and identity providers that had established formal relations and operational agreements in order to engage in transactions with their service users.

GUIDE took as its starting point the existence of a number of these federations and circles of trust that had been created for different administrative and commercial stakeholders, in accordance with the recommendations of the Liberty Alliance [7], which would provide a framework for development of the legal and contractual agreements necessary to create the relations that would serve as the foundation of the circle of trust. Based on these ideas, many EU member states began developing such federations and creating large circles of trust at a national level. However, in most cases these federations were created in isolation from one another. The objective of GUIDE, accordingly, was to define an architecture that would enable a union of these federations in a major circle of trust with the aim of facilitating a single identity environment throughout the European Union.

As we can see, this would be a pan-European federation of identity federations that might also be described as an identity network. The essence of this solution lies in the provision of a circle of trust between member states of the EU for the execution of identity-related transactions through the use of specific entities called GUIDE Gateways. These entities act as interconnection devices between different national circles of trust based on different identification technologies, and can be seen as the forerunners of subsequent solutions like that proposed in Secure idenTity acrOss boRders linked (STORK) project [8].

In 2005, at practically the same time as the GUIDE proposal, a pan-European structure was proposed that was also based on a federated model using at least one, possibly more, identity portals in each member state. These trustworthy portals were responsible for both authenticating entities at a national level and for deciding what level of trust must be assigned to different authentication procedures performed in each member state.

In this model, called the Modinis Conceptual Framework (see Fig. 2) and developed in the Modinis IDM Study [9], the authentication requirements for a specific service in a member state would accept as equivalents the authentication levels and mechanisms used in another state, in accordance with a series of established common criteria. The main contribution of the project is its presentation of a viable pan-European Identity Management System that is notable for being a federated and technologically neutral model that allows pre-existing national systems to join. Modinis does not require a specific pan-European infrastructure.

Modinis is a purely conceptual study that begins from the premise that certain issues like authentication and sources of reliable data regarding the identity of entities will be defined and implemented

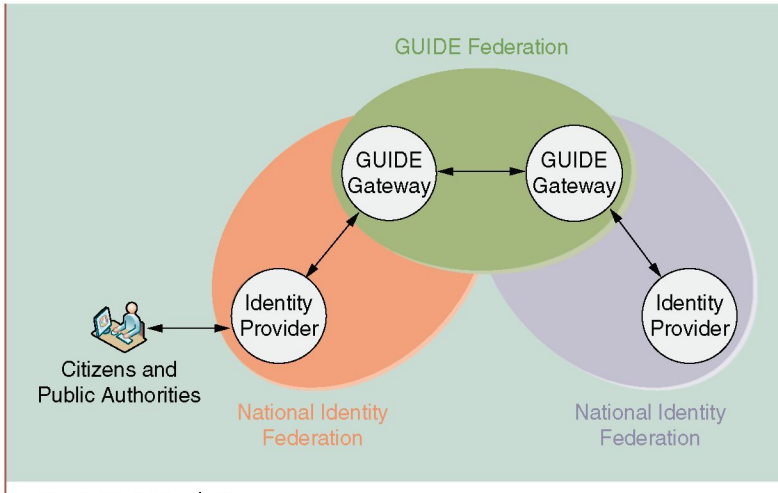

Fig. 1. GUIDE solution.

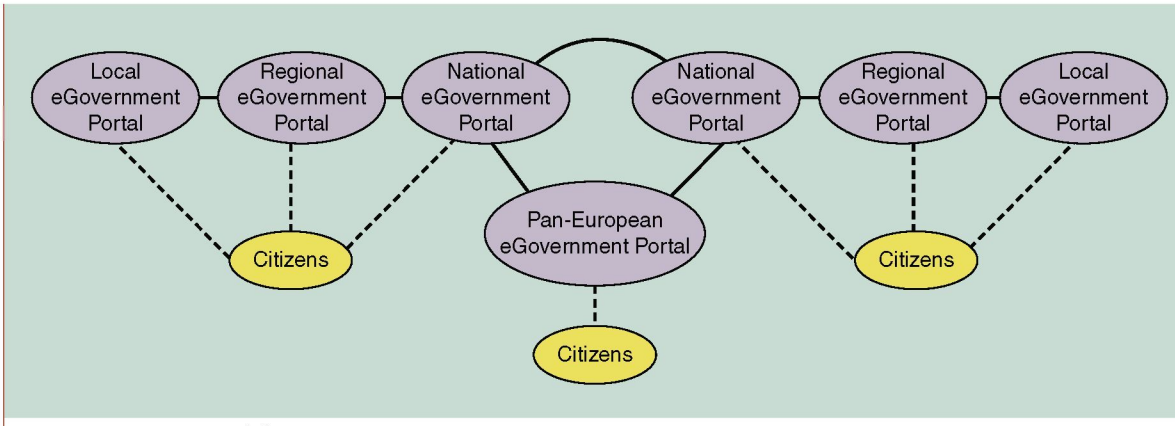

Fig. 2. MODINIS model.

at some point in the future. This means that Modinis does not specifically address practical, technical problems like the definition of levels of trust or semantic interoperability. Instead Modinis postpones solutions to some of the more complex issues. As we will see, these more complex issues will be dealt with later by the STORK project [8].

The year 2007 was important from the point of view of interoperability. In 2007 the European Union set out a roadmap [10] for establishing a series of design principles of IDMs that would be applicable to all member states. Shown in Table I, these principles rely on the fundamental principle of subsidiarity: that each member state must preserve its own autonomy and responsibility to continue to pursue initiatives in identity management systems.

From the technological point of view, it is relevant that the characteristics of pan-European Identity Management Systems are established in consonance with proposals developed to date, with a series of criteria to be verified by IDMs, both from a national perspective and in terms of their relations with other member states.

Also in 2007, the IDABC [11] proposed, in a project called eIDInteroperability for Pan-European eGovernment Services (PEGS) [12], a general architecture for pan-European eIDM. Unlike the other proposals, the IDABC proposal preserved the content of the roadmap for a European framework on interoperability [10], seeking to meet established technology requirements. This work yielded a high-level description of a federated model for interoperability that was technologically neutral and supported multiple authentication levels. This model set the standard for the development of an ambitious project called STORK [8] that began in 2009, and has taken into account the proposals of IDABC and continued progress in its applicability.

STORK is based on the existence of proxies that, in a similar way to GUIDE Gateways, act as interconnection devices between different national eIDMs. Further, this model requires the creation of national Identity Providers (IDPs) (at least one per country) joined in the proxy

Table I
Design Principles of IDMs Established in Roadmap [10].

Usability must be the most pervasive design constraint.
Each member state should be able to identify users within its borders.
Each member state should issue the means to each user to identify and authenticate themselves electronically.
With regard to mandate/representation authorizations, each member state should provide the means to manage the competences of the identified users within its borders.
Each member state should support online validation mechanisms of identities, competences and mandates.
High-level consensus must be established between member states on an eIDM terminology in order to guarantee conceptual/semantic interoperability.
There must be mutual trust between the administrations of different member states in identification and authentication methods.
Member states should be permitted to provide multiple security levels for eIDM services, with criteria defined at a European level for each authentication level.
A single authentic source should be available for each piece of data regarding each registered entity in the member state of origin, thus eliminating duplication of data and ensuring a single correct and official source.
Enabling private sector uptake, where member states choose to rely on private sector partners for the provision of eIDM services.

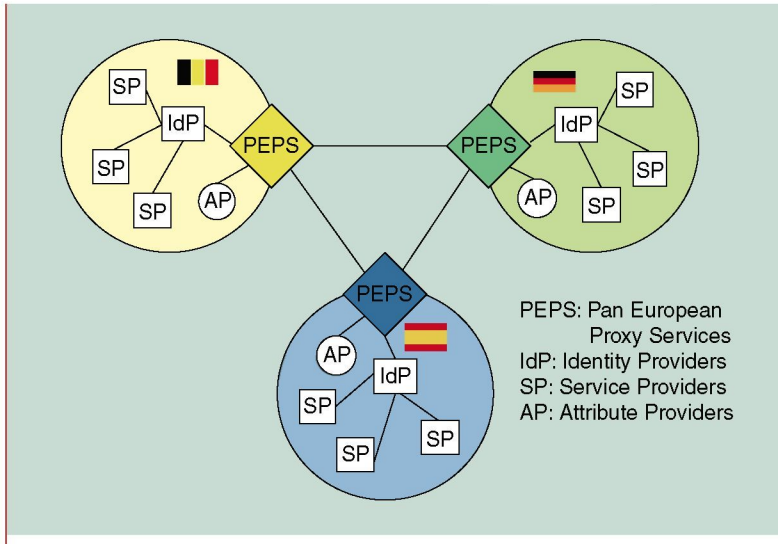

Fig. 3. STORK solution.

network. These proxies, called Pan European Proxy Services (PEPS) would be created at a national level, although the model also envisages the possibility of a centralized European proxy or even a mixed model in which some countries would rely on national PEPS while others would use a European PEPS (see Fig. 3). Moreover there are virtual IDPs (V-IDPs) in the STORK architecture. V-IDPs act as intermediaries between PEPS and existing middleware solutions already in place in some states (Austria, Germany, etc.). The STORK middleware interacts with service providers (SPs), where authentication requests and responses are exchanged.

PEPS are useful mainly in overcoming a technical problem that arises when a broad range of identification/authorization solutions exist for access to services, as is the case in the European scenario. Hence, the STORK model defines four Quality Authentication Assurance (QAA) levels [13], where the lowest level of assurance or QAA would correspond to electronic identifications solutions based on users and passwords, while the highest level would be through an electronic certificate with an eID or smart card. The definition of levels takes into account both the organizational and technical component of each solution. The QAA levels defined are similar to those described by IDABC and are compatible with those defined in work on electronic identity assurance by Liberty Alliance. On the basis of these levels, national identity solutions can be mapped into previously defined and agreed patterns, thus allowing the STORK model to be applied in all countries, regardless of identification systems these allow. Fig. 4 shows the European circle of trust created between participant countries in the pilot phases of the STORK project, along with the authentication assurances allowed in each.

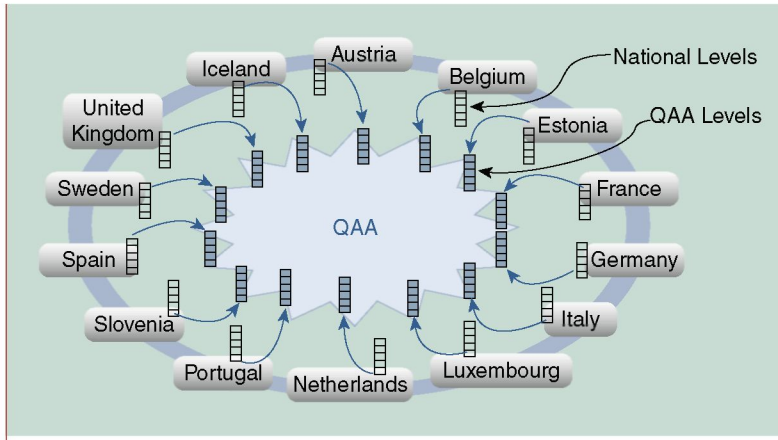

Fig. 4. QAA and circle of trust among PEPs.

Hence, if different QAA are allowed in accessing a service, the technical infrastructure should be able to support them. This is where the PEPS come into play. Their main function is to connect service providers with the proper identity providers in each country – redirecting authentication requests to the pertinent IDP – and to validate the trust and security of the identity information sent by identity providers. Thus, all the PEPS will form a circle of trust in accordance with the solutions specified by Liberty Alliance [7].

The use of Security Assertion Markup Language assertions is suggested for the transport of identity attributes from identity servers to service providers through PEPS, and HTTP Post Binding and Web Browser Single Sign On for redirections and session maintenance. The STORK project seeks to rely on, as far as possible, open standards, and it provides a solution to interoperability at a pan-European level that does not require any modifications in national eIDMs. Thus, STORK takes into account the use of all models of identification/authorization now deployed in member countries of the European Union.

Future Trends

Bearing in mind all the models presented and adhering to the recommendations contained in the European roadmap [10], the way to achieve interoperability will use federation and will be multi-level. All solutions presented have a federated infrastructure that can separate the provision of the service from the identity-related processes necessary to provide the service: user registration, generation and storage identity, and authentication data. The fact that the system is also multi-level facilitates the uptake of all countries with their own digital identities and eIDMs with no significant infrastructure changes, at least in principle, thus speeding up the implementation of a pan-European Identity Management System.

Other aspects to emphasize, common to several of the solutions (MODINIS, IDABC, and STORK) are the ability to operate without having to deploy a European-level infrastructure and the facility to incorporate into the system quickly and easily when needed for less technologically developed countries. Achieving a total integration that would facilitate joint European growth will require the capability of simple and non-onerous uptake, in both economic and technological terms, on the part of countries with more limited means, as envisaged in solutions such as those proposed in IDABC and STORK. A centralized element can be used (a central PEPS) capable of meeting the demands of countries that, owing to various circumstances, have been unable to deploy their own infrastructure.

In spite of the series of solutions presented in this paper, interoperability in identity management remains a challenge. Solutions based on federation resolve a number of problems and are now being presented as the path to follow. A good example of this is the STORK project. After the end of its pilot trials, STORK received funds from the ISA program [14] to extend the solutions attained and ensure their sustainability, as shown in [15, section I, part 1, annex], of the ISA Work Programme.

Nevertheless, a series of doubts have emerged about both the technology and the citizens and, mainly, their integration. Are solutions like STORK viable in the short term? And more importantly: Are they sustainable and in line with present technology in identity management? The latter question generates the most uncertainty and it is related mainly to integration of identity technologies in society and their application to everyday life.

One traditional demand of citizens is to have a "single" identity that is integrated in the network. That is, a single credential that will enable them to access all services offered by a given service provider independently of whether the provider is the government or not and whether the services are public or private. In the same sense, the criteria arising from the European roadmap [10] mentioned above include the uptake of the private sector in eIDM solutions. Integration of private enterprise in pan-European Identity Management Systems is a major challenge both technologically and socially, especially with regard to small and medium-sized enterprises, which have fewer resources and less specialized personnel. Present proposals barely address possibilities for integration with industry, and instead offer solutions solely for interoperability in the private sector.

How can such solutions integrate with the identity environments most commonly used in industry? From the viewpoint of the authors of this article, this issue has received little attention, and today there is little integration between the public and private sectors in identification. There are few service provision environments that make use of the available public eIDMs in the same country. If integration is so insufficient between entities and governments in the same country, where since data custody and information protection is regulated and legislated according to the same criteria there should presumably exist a certain degree of trust – it would seem unlikely that cross-border identification and authentication solutions such as those proposed will be adopted for the provision of services in the private sector.

With regard to the possible alignment of present solutions with future technology trends, the viability of the solutions proposed depends on the path followed in service provision by public administrations. Present trends are pointing towards cloud computing and the provision of services in the cloud. There are European-level studies, such as "The future of cloud computing. Opportunities for European cloud computing beyond 2010" [16] that contain statements such as: "Clouds could assist greatly in the e-government agenda by providing information in one place to the citizen, together with software to manipulate the data." In addition, a number of governments in the world have defined plans and projects to move their services to the cloud. Take, for example, the United Kingdom and its G-Cloud Programme [17], which is led by the Cabinet Office and which aims to achieve a cloud computing infrastructure that will enable public bodies to select and host ICT services from a secure, resilient, and cost-effective shared environment. Outside of Europe, we encounter initiatives like those of Japan or the United States. Japan, through its Digital Japan Creation Project (ICT Hatoyama Plan) [18], is including among its sub-strategies the creation of the Kasumigaseki Cloud, which will enable various ministries to

collaborate to integrate and consolidate hardware, create platforms for shared functions, and provide secure and advanced governmental services. In the United States, there are examples such as USA.gov, one of the government websites that has migrated its resources to the cloud [19].

This move to the cloud poses new challenges in identity management. In an initial approximation that would seem to consist, in the medium term, of the definition of isolated clouds for each of the governments providing services, the STORK project may become viable and applicable with a set of minimal modifications. As we have seen, present eIDMs and service provision environments now constitute independent islands managed by a certain public administration or country. STORK proposes an interoperability solution for these islands. If the islands become clouds, that would not, at first glance, appear to pose greater problems for the solution, which would interconnect and ensure interoperability between clouds by means of proxies.

Although pan-European Identity Management Systems are technologically viable, it must be borne in mind that interoperability in identity management is not just a technological problem. There are significant privacy concerns and legal barriers affecting cross-border and cross-sector relations, and the EU should provide the appropriate legal support before the desired interoperability can be achieved. As the transformation of public administration progresses and private sector business models are incorporated, interoperability in identity systems will become a reality and citizens will play a part in it.

Author Information

The authors are with the T>SIC Group, DIATEL, Polytechnic University of Madrid Ctra. Valencia Km. 7, 28031, Madrid, Spain. Email: {sergio, agomez, belleboni, ipau}@diatel.upm.es.

References

[1] "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - eEurope 2005: An information society for all," May 28, 2002.

[2] "Communities, Commission of the European. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions," in *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All,* Apr. 25, 2006; http://ec.europa.eu/idabc/servlets/Doc?id=25286.

[3] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions," in *The European eGovernment Action Plan 2011-2015. Harnessing ICT to Promote Smart, Sustainable & Innovative Government,* Dec. 15, 2010, p. 743.

[4] European Parliament and Council, "Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC)," *J. European Union,* vol. L 181, pp. 25-35, May 18, 2004.

[5] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions." Aug. 26, 2010.

[6] GUIDE project, *Creating a European Identity Management Architecture for eGovernment;* http://istrg.som.surrey.ac.uk/projects/guide/overview.html, accessed May 29, 2009.

[7] Kantara Initiative, *Liberty Alliance Project*; http://www.projectliberty.org, accessed Aug. 30, 2012.

[8] STORK, Secure Identity Across Borders Linked, cited May 23, 2009; http://www.eid-stork.eu.

[9] The ModinisIDM Study Team, "Modinis-IDM: A conceptual framework for European IDM systems," Sept. 18, 2006; https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ConceptualFramework/2006.09.18.Modinis_Conceptual_Framework_1.1.pdf.

[10] *A Roadmap for a pan-European eIDM Framework by 2010.* vers 1.0; http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf.

[11] IDABC: Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens, cited May 19, 2009; http://ec.europa.eu/idabc/en/home.

[12] J. Majava and H. Graux, "IDABC European eGovernment Services," *eID Interoperability for PEGS: Common specifications for eID interoperability in the eGovernment context.* [Online] Dec. 2007; http://ec.europa.eu/idabc/servlets/Doc?id=30989.

[13] B. Hulsebosch, G. Lenzini, and H. Eertink, "D2.3 - Quality authenticator scheme, Mar. 3, 2009.

[14] Interoperability Solutions for European Public Administrations - ISA Programme. [Online] European Commission. [Cited: May 1, 2011.]; http://ec.europa.eu/isa/index_en.htm.

[15] European Commission - ISA. ISA Work Programme - 1st revision 2011. [Online] Jan. 2011; http://ec.europa.eu/isa/workprogramme/doc/isa_wp_first_revision_2011.pdf.

[16] *European Commission - Information Society and the Future of Cloud Computing - Opportunities for European Cloud Computing Beyond 2010.* [Online] Jan. 26, 2010; http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf.

[17] U.K. Cabinet, G-Cloud Programme. [Online] [Cited: June 3, 2011.]; http://www.cabinetoffice.gov.uk/resource-library/g-cloud-programme-phase-2.

[18] *MIC Announces the Outline of Digital Japan Creation Project (ICT Hatoyama Plan).* International Policy Division, Global ICT Strategy Bureau Ministry of Internal Affairs and Communications (MIC). 1, Tokyo : Ministry of Internal Affairs and Communications (MIC), *MIC Communications News,* vol. 20, pp. 11. Apr. 24, 2009; http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/NewsLetter/Vol20/Vol20_01/Vol20_01.pdf. ISSN 1349-7967.

[19] J. Staten, "Case study: USA.gov achieves cloud bursting efficiency using Terremark's Enterprise Cloud. [Online] Sept. 25, 2009. [Cited: June 3, 2011]; http://www.terremark.com/uploadedFiles/Industry_Solutions/Federal_Government/Case%20Study-%20USA.gov%20Achieves%20Cloud%20Bursting%20Efficiency%20Using%20Terremark%27s%20Enterprise%20Cloud.pdf.

[20] European Commission, "Electronic interchange of data between administrations: IDA programme," [Online] http://europa.eu/legislation_summaries/information_society/strategies/l24147a_en.htm.