Collaboration and the Knowledge Economy: Issues, Applications, Case Studies
Paul Cunningham and Miriam Cunningham (Eds)
IOS Press, 2008 Amsterdam
ISBN 978-1-58603-924-0

The Architecture of an Interoperable and Secure eGovernment Platform Which Provides Mobile Services

Silke CUNO[1], Yuri GLICKMAN[1], Petra HOEPNER[1], Thanos KARANTJIAS[2], Milan MARKOVIC[3], Maximilian SCHMIDT[1]
[1]Fraunhofer FOKUS, Kaiserin-Augusta Allee 31, 10589 Berlin, Germany
Tel: +49 (0) 30 34638000, Fax: +49 (0)30 34638000,
Email: silke.cuno@fokus.fraunhofer.de, yuri.glickman@fokus.fraunhofer.de,
petra.hoepner@fokus.fraunhofer.de, maximilian.schmidt@fokus.fraunhofer.de
[2]*University of Piraeus, Karaoli & Dimitriou 80, Pireaus 18534,*
Tel: +30 210 414 2270, Fax: +30 210 414 2006, Email: karant@unipi.gr
[3]*Mathematical Institute of Serbian Academy of Sciences and Arts, Kneza Mihaila 36, 11000 Belgrade, Serbia, Tel: +381 113770187, Fax: +381 1 18610, Email: mmarkov@beotel.yu*

Abstract: Interoperability and security are considered to be the most important ICT European policy objectives. They are directly addressed in this paper, which describes an innovative architecture designed to build a public administration platform accessible from different countries. Options for the interoperable and secure electronic mobile exchange of public sector documents among and between EU and non-EU regions are outlined. The initial implementation results of this secure, interoperable, open and affordable platform architecture upon which cross border government services are built will be presented. The implementation described is carried out within the EU IST international cooperation project SWEB (Secure, interoperable cross border m-services contributing towards a trustful European cooperation with the non-EU member Western Balkan countries) [1].

1. Introduction

The formation of a common European economical and political space is causing an increase in the migration of human resources across Europe and as a result there is a corresponding necessity to provide public services for EU citizens in all European countries. Governments around the world are working towards integrating existing ICT systems in order to provide them as eGovernment solutions. Those solutions will be forced to interoperate on the local, state, national or even pan-continental level in the close future. Interoperability is therefore the main challenge for efficient information exchange over heterogeneous technology and organizational domain boundaries and is a key component needed to achieve pan-European communication of enterprise systems.

Additionally mobile services are requested in this context. It is assumed that they will contribute towards the solution of demanding pan-European difficulties such as secure exchange of municipal documents and need to be considered with the highest priority. Besides the impressing penetration rates of mobile networks give the unique opportunity to all countries to use mobile services and accelerate their entrance in the digital society.

This paper addresses these topics outlining new and advanced options for the interoperable, secure and mobile electronic exchange of public sector documents. An innovative platform covering actual demands regarding interoperability issues is presented. The platform provides an open and affordable government enterprise solution, upon which

secure cross-border mobile government services can be built. It is based on Web services technologies that will realize a Service Oriented Architecture (SOA) for governmental applications, supporting mobile access and taking into account specific and demanding security requirements. Within this implementation two specific municipal services were tested:

- Residence Certification Service: as a specific example for a secure municipal document exchange service, in which a public organization and individual citizens can securely communicate e/m-municipal documents.
- Electronic/Mobile Invoicing, which has a critical role in all the stages of handling Value Added Tax (VAT) procedures for EU Member States. Through e/m-invoicing, tax administrators will be able to implement new tools and procedures to carry out alternative controls.

The platform was implemented within the EU IST international cooperation project SWEB.

2. Background and related work

Centralized eGovernment approaches, such as web portals did not succeed in addressing needs such as interoperability with back-office systems that operate in Small and Medium Governmental Organizations (SMGOs). Likewise they did not guarantee security and trust, which are key enablers of current digital governmental environments, based on many interacting objects, devices and systems. And thirdly they did not meet the demands on scalability and extensibility since e/mGovernment enterprise solutions due to their increased usage in everyday life, need to be simple, open and reconfigurable, providing easily reengineered services and taking into account that the large number of citizens needs also to be served with acceptable quality of service levels. Indeed the major focus of centralized e-Government approaches was to be built upon content distribution and to embed the business logic of all services directly into the various enterprise applications.

The RISER (Registry Information Service on European Residents) - service [2], supported by the EU's eTEN programme, was the first cross-border eGovernment service through a central web portal. RISER has established an Internet based platform with eServices, addressing governmental organizations, citizens and companies to facilitate the creation of a more citizen-centred form of government. It focused on the protection of personal data and the security of the entire system, influencing current SWEB-considerations, even if it adopted all the drawbacks of similar centralized eGovernment approaches that were analysed previously.

Extensively used distributed eGovernment solutions did not succeed to achieve their premises due to the lack of standardized, open source technologies in building advanced content repositories, middleware messaging systems, customizable content management systems, business process management systems, strong security mechanisms and interoperable modules, at the time that these solutions were deployed. However, today the open-source world appears mature to provide stable technology premises and to build real interoperable and secure enterprise systems.

The eMayor-project [3] is the predecessor of the SWEB-project, a 6th framework research project (2004-2006), in which five municipalities tested two secure cross border eGovernment services using an advanced platform as the basis for the development of new municipal services. SWEB partially takes on the residence scenario-case from RISER and reuses results of the eMayor project making architectural changes/updates to the eMayor platform. However, several enhancements were required in order for the eMayor platform to be adopted in the governmental sector. These enhancements involve the architectural structure of the platform, which was needed to be redesigned appropriately in order to be

based on SOA technologies and frameworks, extending the security mechanisms supported and the scalability of the solution.

The fact that the mobile aspect is partially covered in all the above mentioned - existing government architectures, and that many technology frameworks and tools used for their integration are not supported in our days, imposes their replacement with more synchronous ones. Besides, mobile requirements for service and technology interoperability, strong security, user-friendliness and low cost, overcoming bandwidth and performance considerations, as well as existing development difficulties, increase the need of introducing new, more completive frameworks. These shall be designed and consisted from advanced, independent modules that will be able to provide high administrative e/mServices with one, single implementation.

3. The Technical Architecture

3.1 Architecture overview

The innovative design of the proposed architecture aimed to achieve interoperability among SOA platforms as well as with the back-office systems and independent applications that operate in the governmental organizations, expandability of its functionality and high level of quality by means of system security and privacy. This is realized by using advanced XML-technologies, PKI, XML-cryptography and design methodologies, resulting in an elaborate platform that fulfills all requirements to join up with needs of governments, offering a trusted environment to citizens at the same time.

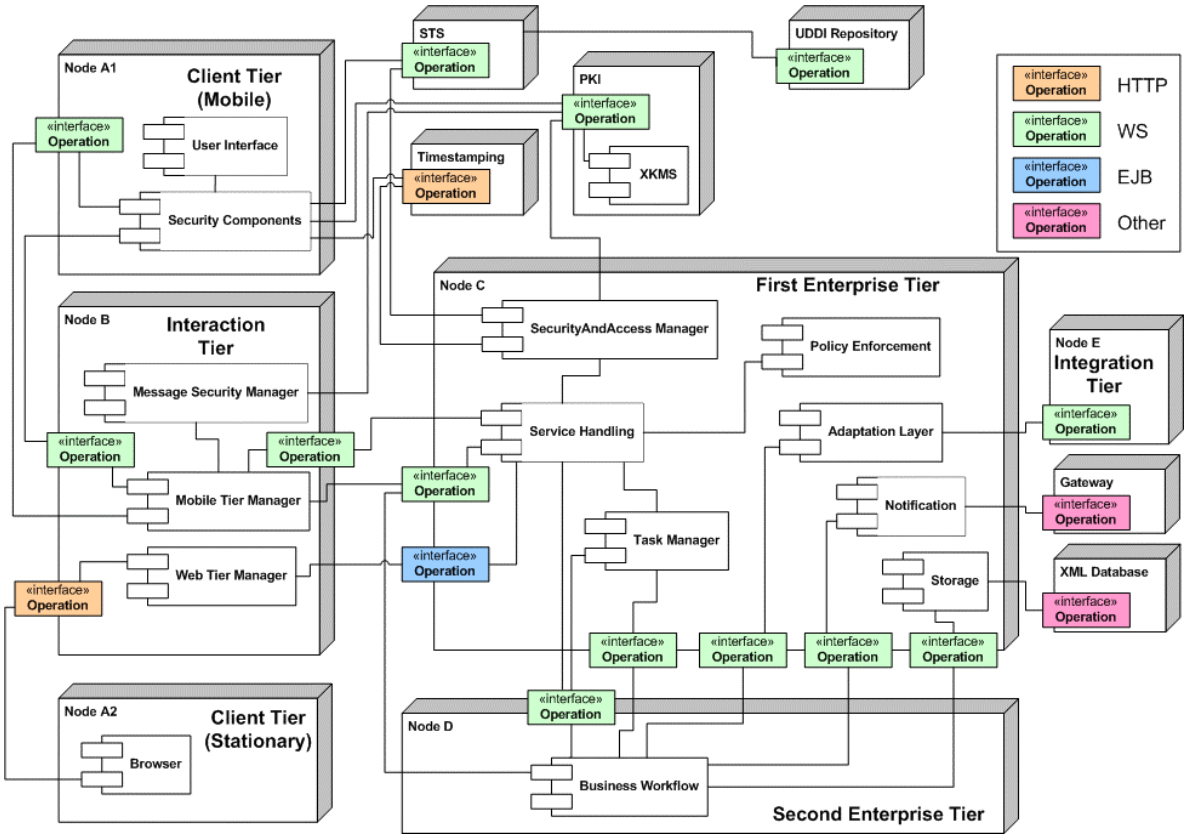

Figure 1. SWEB platform components

The architectural overview of the presented SWEB platform, as depicted in Figure 1, consists of several concrete tiers, which are listed below and focus on achieving all the requirements mentioned above:

1. The client tier (Node A), which holds the components necessary for the user to access the system.
2. The interaction tier (Node B), which includes all the components that are directly used to communicate with the platform such as the Mobile Tier Manager - for accessing the SWEB platform using mobile devices and Web Tier Manager - for accessing the SWEB platform using a standard conform browser and smartcards.
3. The first enterprise tier (Node C), which holds all basic services and the platform core such as the Service Handling – for communicating between the Interaction Tier and other basic components at the First Enterprise Tier, the Security and the Access Manager – for implementation of all security features on the platform as well as for user authentication, the Policy Enforcement – for achieving user authorization on the SWEB platform, the Task Manager – for managing all tasks and service related documents, the Notification – for creating and sending notification messages to users, the Storage – for permanently storing requests (like e/m-Invoices) by using the XML-database, and the Adaptation Layer – for communication with the legacy system of the governmental organization.
4. The Second Enterprise Tier (Node D), which contains the actual business services and is realized using Business Process Execution Language (BPEL) [7] for service orchestration, organizing the embedded logic of an application into separate and easily changed "state machines". This allows new levels of processes to be defined within businesses, fulfilling the compartmentalized needs of different GOs departments and providing scalability and extensibility with minimum effort.
5. The Integration Tier (Node E) where the actual legacy components reside.

Besides, there are several external systems providing external services, such as:

1. A brokered Authentication Server for user authentication and authorization by issuing SAML (Security Assertion Markup Language) tokens which are required for users to be authenticated and authorized on the main enterprise platform.
2. A TimeStamping server for issuing time-stamping tokens in order to achieve non-repudiation, which is a mandatory security requirement when dealing with governmental organizations.
3. Public Key Infrastructure (PKI) services, which provides all the required cryptographic credentials in the presented framework, such as X.509 digital certificates.
4. A UDDI repository that stores URLs of the SWEB-enabled municipalities.

One of the major achievements of the platform is the advanced functionality provided in accessing governmental services with the use of mobile devices. Consequently, the design and realization of the mobile client components were of special importance. Our try was to provide a mobile framework rather than implementing a specific mobile application that could be used only for the premises of a project. The designed and implemented framework comprises of four core capsules, as depicted in Figure 2, the functionality of which should be included in every future mobile implementation that is intended to be used in advanced governmental frameworks.

Specifically, the Web Services Capsule implements all formulation and handling mechanisms of the transmitted messages to external communicating entities (Request Handler). It actually encloses all clusters of data into Web Services, integrating as well the reception and extraction of the main body mechanisms (Response Handler) on every other end of communication.

The Interface Capsule implements the transition between m-forms (Form Handler) during the process of user interaction, the selection and automated adjustment of language and character set on these forms (Language Component), and the transformation of the given data into a format compliant with the adopted mGovernment XML schemas (Transformation Component).

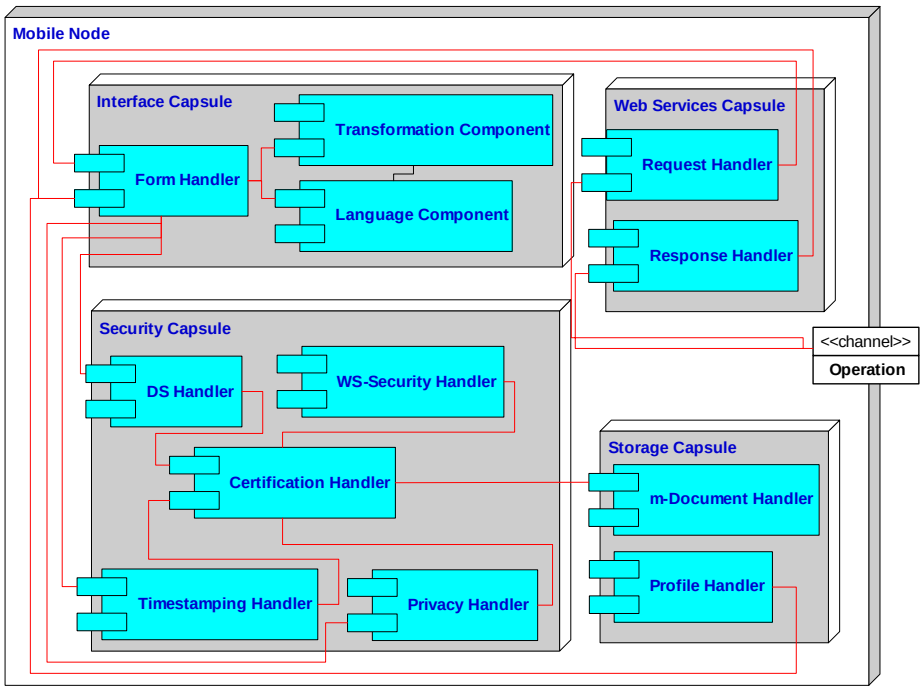

Figure 2. Mobile Node - Client Tier Analysis

The Security Capsule integrates strong security mechanisms on the mobile device. It creates and verifies XML-digital signatures on the m-documents (DS-Handler), which are automatically structured from the m-forms, as well as the hash values of the signed m-documents and requests for valid timestamps (Timestamp Handler) from the TSA. All SOAP messages are digitally signed and encrypted (WS-Security Handler) using strong cryptographic credentials, which are stored and handled in this capsule (Certification Handler). Furthermore, it creates the appropriate requests for obtaining valid authorization tokens from the brokered Authentication server (Privacy Handler), receives and handles them by automatically embedding them in messages to be sent to the main e/mGovernment platform.

Finally, the Storage Capsule stores and handles the created and received m-documents (m-Document Handler) and the various profiles of users (Profile Handler) on the mobile device. Depending on the authenticated user, many fields (ex. name, surname, V.A.T. number, etc), of the m-forms are automatically fulfilled.

3.2 Interoperability Aspects of the presented SWEB platform

The synchronous enterprise SOA platform, presented in this paper, is designed to provide cross border municipal government services to the citizens of EU and to the citizens of other European countries that are going to join EU in the future. Such services require strong cooperation between the involved municipalities. For successful functioning of the cross border services the interoperability between the municipalities needs to be achieved on all three levels: organizational, semantic and technical.

The organizational interoperability concerns here mostly the interoperability of business processes adopted in municipalities. Usually, these processes have much similarity and simultaneously significantly differ from each other. In the last years numerous efforts to standardize these processes have been done at national and European level. However, the existing differences in legislation, political structure, bureaucratic traditions, cultural and language barriers make this task unattainable for the nearest future. Therefore, the presented platform does not rely on the interoperability of the business processes. Instead, it uses

many of these processes as external services, which have to be individually integrated with the main enterprise platform.

Besides the technical interconnection of large enterprise frameworks, built upon different technologies and platforms, has never been a trivial task [5]. Our platform addresses this interoperability problem [6] by implementing main components as atomic, self-contained Web Services, orchestrated with BPEL, into business processes. As a typical e/mGovernment system it relies upon e-document exchange, which takes place between the internal components of the platform and between the platform itself and the various back-end systems that operate at the governmental organizations. The study performed when gathering the needs and requirements of governmental organizations demonstrated that they have different requirements to the structure of the business electronic documents. Therefore, in order to avoid semantic problems a universal format has been used for all communication between organizations and end users. This format is called sUF (SWEB-universal format) and is used in all components derived from the presented platform. Furthermore a second format was defined, called sMF (municipality format), which corresponds to the format used by the informational system of a municipality. It is assumed that for integration of the platform with the other back-end systems is required a component able to accept sUF and to transform it into sMF and vice versa.

Web Services and advanced XML-based technologies promote the concept of atomic, self-contained, services in the platform, which are accessible and available to a multitude of applications in different and demanding environments, offering the promise and hope of integrating these applications in a seamless fashion [8]. Moreover, all schemas for sUF documents are defined on the basis of the existing initiatives for the business electronic documents such as e-Gif [9] and UBL 2.0 [10] from OASIS. The data structures for the basic concepts used in governmental electronic documents were adopted from these initiatives.

3.3 Security Aspects of the presented SWEB platform

Security and trust are key enablers in our digital governmental environment, based on many interacting objects, devices and systems. Although Web Services permit enterprises to create interoperable services-based applications, their original definition didn’t include a built-in security model [11] in which we had to work on.

The use of the Secure Socket Layer (SSL) [12] protocol to protect communications among service endpoints does not provide the granularity and flexibility, required for more advanced Web Services scenarios, where the endpoints might not have a direct channel to each other. Therefore, the security model of the presented platform is based on many modern security standards and technologies such as the following.

- Second generation PKIs and advanced XML-cryptography mechanisms support a large-scale deployment of a number of security services, such as origin authentication, content integrity and confidentiality, and non-repudiation, establishing trust chains at local, national and international level.
- OASIS WS-Security (WS-S) [13] defines and standardizes a core specification for securing SOAP-messages, plus several extensions for integrating user or service identity information within these, based on XML cryptography. W3C XML-Digital Signature (XML-DSIG) [14] standard defines the appropriate way for rendering digital signatures in XML, making them human-readable, easily parsed, platform independent, and generally more advantageous for workflow environments than preceding standards like the Public Key Cryptographic Standard #7 (PKCS#7) [15]. Correspondingly, W3C XML Encryption [16] standard allows the selective encryption of arbitrary portions of XML documents, allowing seamless integration into workflow processes.

- The use of a brokered authentication system, which issues XML-based security tokens, integrating the Web Services Trust (WS-Trust) [17] standard, enables user authentication in heterogeneous environments providing authorization and auditing advanced mechanisms [18].

4. Business Benefits

The presented platform and all external security services gave us an opportunity to design and implement something innovative in the governmental sector as well as to test and validate new prototype technologies, ensuring their applicability to non-advanced technological infrastructures and their dissemination to other IT communities for potential redeployment and broad application. For executing the cross-border trial scenario Western Balkan municipalities were chosen for collaboration with EU-municipalities.

Our decision was based on the fact that the deployment of eGovernment services has accelerated in the Western Balkans region over the last few years. At the same time, the penetration rate of mobile devices in the region is twice as much as the fixed lines penetration. Consequently, mobile services are very popular in the region and user satisfaction with these services is high. These trends give a good basis for development and deployment of mGovernment services in this area.

According to our expectations the deployment of mGovernment services on the basis of the platform presented in the current paper will contribute to improving citizens' quality of life by making governmental services easily accessible though already widely used mobile infrastructure. With the adoption of the presented secure, interoperable, open and affordable platform and the built upon it secure e/mGovernment services the governmental organisations increase their efficiency, reduce their operating costs, throughput time and improve their quality of service and reputation. Other visionary outcomes of our work lie in bringing in information concerning state of the art on secure Web services for e/m-Government in the European public sector standardization bodies. Furthermore, our approach focuses on setting up the requirements for secure mobile government for governmental organizations, developing guidelines for investors and venture capitalists. The project raised the interest of local mobile network operators as a potential business case and encouraged their involvement.

5. Conclusion

Our solution contributes to the transition process that European Union is currently undergoing on its way to entering the digital society. This overall process includes reorganisation as well as the modernisation of governmental administration processes, the modernisation of the science and technology sector in general including the introduction of cross-border e-services. In this context we managed to design and implement standard-based and advanced security mechanisms and an innovative mobile Web Services framework that can be used in every future mobile implementation that aims to feature cross-border e/mGovernment services, achieving real technical interoperability with existing back-end systems that operate on these organizations as well as with other SOA-platforms. As semantic interoperability becomes particularly important when public authorities need to exchange information, our solution implements pan-European XML-data structures offered by European XML clearinghouses [19]. The presented platform and the associated services that are demonstrated in municipalities and cities of several EU and non-EU countries, in cooperation with the IST-QualiPSo project [20] will be available as Open Source.

Acknowledgement

This work is being carried out in the context of the IST international cooperation project SWEB (044979). This paper is based on the work performed within the context of this project and the authors would like to acknowledge all SWEB partners.

Disclaimer

This research outlined in this paper has been undertaken with the financial assistance of the European Community. The views expressed herein are those of SWEB Consortium and can therefore in no way be taken to reflect the official opinion of the European Commission. The information in this document is provided as is and no guarantee or warranty is given to state that the information is fit for any particular purpose. The user therefore uses the information at their sole risk and liability.

References

[1] SWEB Project Homepage, http://www.sweb-project.org/.
[2] RISER Project Homepage, http://www.riserid.eu/.
[3] eMayor Project Homepage: http//www.emayor.org/.
[4] Microsoft .Net Compact Framework, MSDN Library, http://msdn2.microsoft.com/en-us/library/ms950380.aspx.
[5] A. Kaliontzoglou, P. Sklavos, T. Karantjias, D. Polemi "A secure e-Government platform architecture for small to medium sized public organizations", Electronic Commerce Research & Applications, Elsevier, vol. 4, No. 2, pp. 174-186, 2005.
[6] European Commission, "European Interoperability Framework For Pan-European eGovernment Services", Office for Official Publications of the European Communities, 2004, http://ec.europa.eu/idabc/servlets/ Doc?id=19528.
[7] OASIS Web Services Business Process Execution Language Version 2.0, WSBPEL 2.0, www.oasis-open.org/committees/wsbpel/.
[8] European Commission, "European Interoperability Framework For Pan-European eGovernment Services", Office for Official Publications of the European Communities, 2004, http://ec.europa.eu/idabc/servlets/ Doc?id=19528.
[9] OASIS Universal Business Language v2.0, Standard, 2006, http://docs.oasis-open.org/ubl/os-UBL-2.0/UBL-2.0.html.
[10] Cabinet Office, e-Government Unit, e-Government Interoperability Framework Version 6.1, 2005, http://www.govtalk.gov.uk/documents/eGIF%20v6_1(1).pdf.
[11] B. Hartman, D. J. Flinn, K. Beznosov, S. Kawamoto, "Mastering Web Services Security", Wiley Publishing, 2003.
[12] T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, 1999, http://www.ietf.org/rfc/rfc2246.txt.
[13] WS-Security Core Specification 1.1, OASIS Standard 1.1, http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf.
[14] XML Signature Recommendation, XML-DSig, http://www.w3.org/ TR/xmldsig-core/.
[15] RSA Laboratories, "PKCS 7 v.1.5: Cryptographic Message Syntax Standard", Technical Note, 1993, ftp://ftp.rsasecurity.com/pub/pkcs/ doc/pkcs-7.doc.
[16] XML Encryption, http://www.w3.org/Encryption/2001/.
[17] WS-Trust Specification 1.3, OASIS Standard, 2007, http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.doc.
[18] S. Papastergiou, A. Karantjias, D. Polemi, "A Federated Privacy-Enhancing Identity Management System (FPE-IMS)", in The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2007.
[19] IDABC, IDABC Semantic Interoperability Strategy: The European XML Clearinghouse, Feasibility Study, December 2005, http://ec.europa.eu/idabc/servlets/Doc?id=24406 and Semantic Interoperability Center at: http://www.semic.eu/.
[20] QualiPSo Project Homepage, http://www.qualipso.org.