Information Polity 15 (2010) 105–123
DOI 10.3233/IP-2010-0199
IOS Press

Semantic interoperability architecture for Governance 2.0

Adegboyega Ojo[a,*], Elsa Estevez[a,b] and Tomasz Janowski[a]
[a]*United Nations University – IIST Center for Electronic Governance, Macao SAR, China*
[b]*Universidad Nacional del Sur, Bahia Blanca, Argentina*

Abstract. The increasing use of social media by governments for improving citizen access to information, participation of stakeholders in policy processes and delivery of customer-focused services are among the defining features of the so-called "Governance 2.0" phenomenon. Another feature is the interaction between existing government networks and social networks of citizens and policy actors in order to disseminate government information and seek contributions from citizens and other actors to policies, decisions and services. This article examines the semantic issues associated with the emerging Governance 2.0 networks. It evolves an architectural framework to guide governments and their agencies in developing semantic interoperability capabilities. We approach the problem by first developing a conceptual model for analyzing semantic interoperability requirements in general. Next, we provide a case study to generate interesting scenarios and identify concrete semantic interoperability issues arising from the interactions between citizens, businesses and government through traditional and electronic channels and different forms of social media. Subsequently, we present a Semantic Interoperability Architecture Framework to address these issues based on existing government semantic interoperability frameworks and semantic standards for Web 2.0. After validating the prescribed framework, we discuss how it could be used in practice by governments.

Keywords: Semantic interoperability, semantic interoperability reference architecture, semantic interoperability and Web 2.0, semantic interoperability in governance 2.0, semantic tags, semantic mashups

1. Introduction

The tenets of modern public policy and management such as service-orientation, devolution of power to core actors in policy networks, and increasing use of non-traditional instruments for policy making and implementation [1] fundamentally requires network forms of governance [2]. Many such networks are of informal nature and outside government control. Enabled by Web 2.0 technologies (Governance 2.0), they potentially provide huge opportunities for government leaders to connect to their stakeholders and learn about their needs.

Web 2.0 technologies exploit Internet connectivity to support networking of people and contents [26]. Their impact on governments includes increased transparency and participation of citizens in decision-making and more collaboration between agencies [3]. Various governments have responded strongly to these opportunities by exploiting social media in engaging citizens and their own employees [4]. Governance 2.0 applications include cross-agency collaboration and knowledge management at the

*Address for correspondence: Adegboyega Ojo, UNU-IIST Center for Electronic Governance, Casa Silva Mendes, Est. do Engenheiro Trigo No. 4, Macao SAR, P.O. Box 3058, China. Tel.: +853 28712930; Fax: + 853 28712940; E-mail: ao@iist.unu.edu.

back-office, and political participation and service provision at the front-office [3], all focusing on communication, interaction and services [4].

The interoperation of intra-government networks with social networks raises significant semantic interoperability challenges in addition to technical and organizational ones. Semantic interoperability is concerned with the ability of interacting elements of a network to use exchanged information in a manner consistent with the intended meaning of such information, particularly in the cases where the information is used outside its original context. Semantic interoperability is a fundamental concern in Governance 2.0 given that most Web 2.0 applications involve the use of data outside their original context.

This paper provides a conceptual framework for analyzing semantic interoperability (SIOP) requirements for Governance 2.0. The framework provides three dimensions for analyzing such requirements: (1) what kind of policy, governance, organizational and technical capabilities are required for SIOP; (2) at which level are the SIOP requirements addressed, e.g. network (whole of government) or entity (individual government agency); and (3) what communication layers – context, protocol, message, contents and domain are associated with semantic conflicts.

To obtain concrete requirements, a case study has been employed to generate interesting scenarios and to analyze them for possible semantic conflicts. Based on the requirements, relevant government semantic interoperability frameworks and emerging semantic standardization efforts for Web 2.0, we prescribe a set of reference architectures to guide government leaders and managers in developing their semantic interoperability capabilities in support of Governance 2.0 initiatives. We also validate the architectures, explain their use, and present general recommendations for implementing them.

2. Background

2.1. Defining semantic interoperability

The notion of Semantic Interoperability (SIOP), though frequently referenced, is seldom explicitly defined in literature. For example [5] describes it as a shared vocabulary and semantics of knowledge exchanged during collaboration, while [6] presents it as the use of ontologies to support negotiation in open systems. At the same time, government interoperability frameworks adopt a broader and more formal view of the concept. For instance [7] defines SIOP as support for coding, transmission and use of meaning between interacting parties across related services (e.g. health), and assigns the attributes of precision, consistency, understandability and reproducibility to semantically interoperable data. In [8], SIOP denotes the ability of entities to share information meaningfully and to engage in meaningful collaborative activities in order to jointly perform business processes. In [9], SIOP is said to be achieved when: (i) data exchange partners have a common understanding of the meaning of the shared data, (ii) data exchanges adhere to the shared understanding, and (iii) data is exchanged without misinterpretation.

Considering the above definitions, we present a consolidated definition for the purpose of this paper as follows:

Definition 1: Semantic Interoperability is the ability of interacting network entities – agency systems, citizens, social media, etc. to have a consistent understanding of the shared information based on the network's ability to resolve differences in the conceptualization of entities and the member's ability to: ascribe meaning to the information they wish to share, discover information they need based on the descriptions provided by others, and process the shared information in a way consistent with the intended the use.

The above definition implies that SIOP capabilities include three core functions:

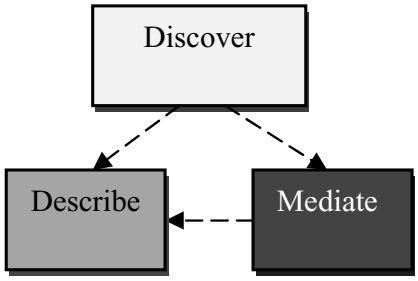

Fig. 1. Core semantic interoperability functions.

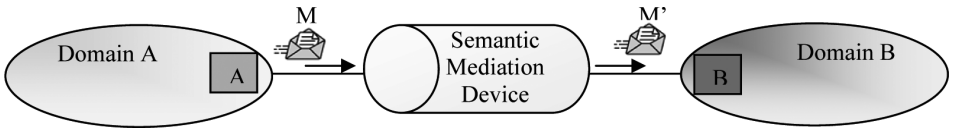

Fig. 2. Abstract representation of semantic mediation.

– *Semantic Description* – describing information assets based on some form of conceptualization;
– *Semantic Mediation* – resolving differences in conceptualization when searching for information assets; and
– *Semantic Discovery* – locating assets based on semantic descriptions.

The relationships between these capabilities are depicted in Fig. 1.

Semantic description capability entails the use of some form of metadata in annotating information assets. This aspect is perhaps the most fundamental and mature of the three. As a result, most Government Interoperability Frameworks (GIFs) already include comprehensive metadata specifications, e.g. [10]. Semantic discovery capability is supported by existing semantic technologies by building on semantic descriptions frameworks.

Semantic mediation is the least developed aspect of semantic interoperability. Its objective is to resolve semantic differences that may arise in the context of information exchange between participants in an interaction, e.g. service delivery. Semantic mediation involves providing translation services to interacting entities from different semantic domains. Figure 2 shows a translation service provided by the semantic mediation device (semantic gateway [11]) to transform a message M from the semantic domain A to an equivalent message M' in another domain B.

The rest of this section highlights the major theoretical frameworks, initiatives and government frameworks aimed at addressing the problem of semantic interoperability.

2.2. Theoretical frameworks

A number of theories have contributed to better understanding of the semantic interoperability problem, five of them highlighted in this section. The first two contribute to understanding the nature of communication, while the remaining three address semantic mediation.

1. *Speech Act Theory* explains the kinds of messages (speech acts) that could be exchanged between two parties [12,13]. According to this theory, speech acts consist of: (i) communication action itself, (ii) the intention behind communication, and (iii) the effect of communication on the parties and the world [13].

2. *Agent Communication* examines how several software entities may communicate with one another. This framework enables assigning meanings to utterances. It indicates that the meaning of a statement depends on [14]: the context in which the statement is uttered, its position in a sequence of previous utterances, the nature of the statement (e.g. commitment or request) and the objects referred to in the domain [15].
3. *Semantic Conflicts* recognize that differences in conceptualization may lead to different types of semantic conflicts in information exchanged between network entities including [11]: (i) different representations for the same value type; (ii) differences in the units or scales of values; (iii) different legal implications for the same data in different contexts; (iv) different concepts described by the same word (homonyms) or multiple words describing the same concept (synonyms); (v) the meaning of data depending on the value of another data; (vi) describing one concept with different sets of attributes; and (vii) data considered correct in one context violates integrity constraints in another context.
4. *Ontology Alignment* – In practice, conceptualizations are formally represented as ontologies – defining and relating concepts relevant to a domain, system or application [16]. Ontology alignment aims at relating concepts belonging to different ontologies or conceptualizations.
5. *Information Flow Theory* provides a sound mathematical basis for semantic interoperability in a distributed environment. The theory addresses SIOP by characterizing syntactic and semantic structures (ontologies) of systems that wish to interoperate and relating these structures across communities [17,18].

Based on these theories, a number of SIOP research projects have been carried out to advance the state of the art in the domain, as highlighted in Section 2.3.

2.3. Semantic interoperability initiatives

We highlight six projects carried out through European Commission's IST program: SmartGov (smartgov.e-gov.gr), SemanticGov (semantic-gov.org) [19], Access-eGov (accessegov.org), OntoGov (hsw.fhso.ch/ontogov), UDEF (udef.com) and ATHENA [20], and Federal Enterprise Architecture Reference Model Ontology (FEARMO) [21].

These projects have produced: semantic descriptions of services, domain ontologies, semantic web service infrastructures for governments, and support for semantic mediation [7]. The outcomes of these projects provide vital inputs into development of Government Semantic Interoperability Frameworks in a number of countries, as described in the following section.

2.4. Government-specific frameworks

We review Government Semantic Interoperability Frameworks (GSIF) from five leading e-government states indicating their purpose and major elements:

FEA Data Reference Model (DRM) – This model helps identify what data the federal government has and how such data can be shared in response to business/mission requirements. It facilitates information exchange within communities of interest and enables credible cross-agency agreements on governance, data architecture and information sharing. The model consists of three areas – data description, data context and data sharing [22].

EU Content Interoperability Strategy – This strategy facilitates semantic interoperability by the use of semantic interoperability assets (SIA) – information resources developed to address semantic interoperability requirements in information systems, such as dictionaries, thesauri, taxonomies, mapping-tables,

ontologies and service registries [23]. Other aspects include developing semantic gateways for translation, clearing houses and registries for managing SIAs, and organizational processes.

UK e-Government Metadata Standard – This standard addresses the maximum consistency of metadata across the public sector. Part of the e-Government Interoperability Framework (e-GIF), it specifies the elements, refinements and encoding schemes for creating metadata [10].

Dutch Interoperability Framework – Aimed at ensuring that information exchanged is meaningful to all parties within a community of interest, the framework prescribes semantic interoperability solutions involving: (i) data definitions; (ii) terminology and controlled vocabularies; (iii) computational models and assumptions for producing results; (iv) conceptual and functional models; (v) business process models; and (vi) policies for access, authentication, authorization, security, transparency, accountability, privacy, etc. [8].

Australian Information Interoperability Framework – The framework describes information interoperability as the ability to transfer and use information in a uniform and efficient manner across multiple organizations and information technology systems [24]. It defines principles underpinning sound information management; establishes concepts, practices and tools that can drive successful sharing of information across government; and identifies six enablers to support information sharing – partnership and collaboration, authoritative sources of information, common business language and standards, governance structures, legal and policy frameworks, and tools.

3. Conceptual framework and approach

We present a conceptual framework for exploring semantic interoperability requirements for Governance 2.0 based on the theoretical frameworks in Section 2.2, and an architectural framework to structure semantic interoperability solutions.

3.1. Generating requirements space

Semantic interoperability requirements analysis is based on three models related to government interoperability, agent communication and collaborative network organizations. The resulting premises for SIOP requirements are:

1. Government interoperability is a multidimensional, complementary, dynamic and context-specific capability [25];
2. The capability is required at the network level [25,26] and individual network member level;
3. Semantic communication between two entities involves a number of communication layers – context, protocol or conversation, message, content and domain description [15]. Consider for instance a request r made by an agency A to another agency A' for family details I of a citizen C, required to process a child benefit for C. The "context" for this communication is the "Social Benefits" service. The "protocol" is a sequence of messages following the request from A e.g. an acknowledgement from A' upon receiving r. The "message" layer refers to the nature of communication, i.e. request for information. Finally, the "domain" layer determines the meaning of objects referenced in the message, e.g. is C an ordinary citizen or a public official of A, and does I mean the spouse and children of C or all dependants of C?

These premises provide different perspectives to exploring semantic interoperability issues. We can therefore define a space for semantic interoperability requirements based on three dimensions (Fig. 3):

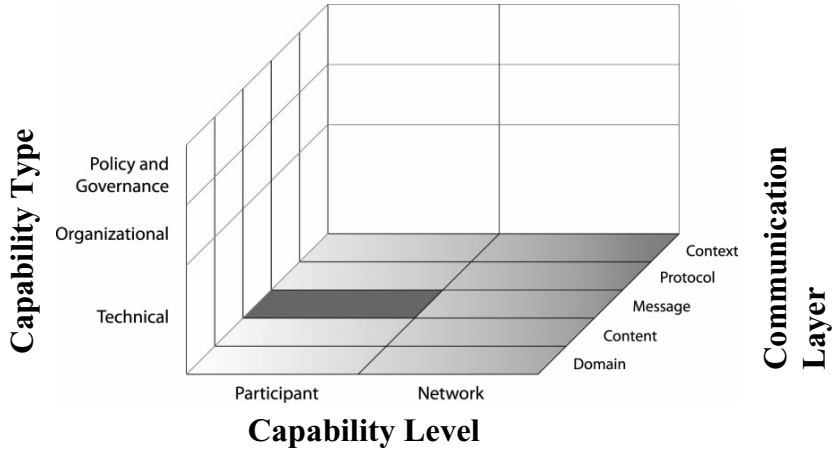

Fig. 3. Semantic interoperability requirement space.

Capability Type, Capability Level and Communication Layer, with specific semantic interoperability requirements identified based on the capability type (e.g. technical), capability level (e.g. network) and communication layer (e.g. context).

For simplicity, we reduce the capability types defined in [25] for both network and participant levels into: policy and governance, organizational and technical. We exploit this capability structure in analyzing SIOP requirements for Governance 2.0 in Section 4.1.

3.2. Architectural elements for semantic interoperability

To deliver a holistic SIOP capability based on the identified requirements at the network and participant levels, an architectural approach is essential, providing multi-perspective and multi-level views to solutions. In order to address the solutions at both capability levels, two complementary architectural models are required: one supports collaborations in networked organizations and communities (network level), and the other supports description of capabilities within an enterprise (participant level). Specifically, we adopt the Collaborative Networked Organization (CNO) model [26] for describing network-level SIOP capabilities. The CNO model provides Structural, Componential, Functional and Behavioral dimensions mapped into:

- Participants – describing members of the community, their information-sharing goals and roles, and responsibilities of each member;
- Resources – shared or joint information, knowledge, semantic assets, information systems and computing infrastructures to enable semantic interoperability at the network level;
- Processes – both primary processes providing context for information-sharing, and auxiliary processes and practices that enable semantic agreements between network members; and
- Governance – rules, contracts, and other established agreements governing the behavior of network members.

At the participant level, the SIOP capabilities are structured through a generic architectural framework [27] which prescribes four domains of architectural concerns to technological initiatives: Contextual, Conceptual, Logical and Physical. We map these generic domains to respective dimensions considering the SIOP capabilities:

– Process – business process context for semantic interoperation;
– Information – information and other enterprise semantic assets required to support semantic-enabled processes;
– Services – major components of solutions (e.g. services and applications) and the required interfaces for providing access to information and semantic assets; and
– Technology – concrete technologies for implementing semantic services and applications, e.g. ontologies and semantic web technologies.

We elaborate on the architectural elements and consolidate the two levels of architecture in Section 5.

4. Semantic interoperability requirements

This section discusses the semantic interoperability requirements arising from the interactions among the core entities in the Governance 2.0 networks. To determine these requirements, we apply a case study covering major interaction patterns, and rely on the conceptual framework in Section 3 to organize and analyze the requirements.

4.1. Analysis

4.1.1. Case study

Suppose an entrepreneur X is interested in starting up a restaurant business in a suitable district in his state of residence. Aware of government restrictions on restaurant and hospitality services for different districts, X takes advantage of a new open government data initiative to access the latest government policy on restaurant services affecting different districts, offered by the licensing office, and demographic data from the statistics bureau of the state. By integrating these two sets with geospatial data from a private organization, X determines the best location for his restaurant, and afterwards applies for a suitable license.

The state licensing office provides information on procedures for obtaining different categories of business licenses on its portal, and disseminates information on regulations, policies and public notices to citizens and businesses through social network and micro-blogging sites. The agency also harvests contributions from its customers on these sites, related to service experience as a basis for improvement and feedback on policy issues. To process a restaurant license application, the licensing office collaborates with the agencies responsible for building construction, fire services and health care.

4.1.2. Scenarios for exploring Governance 2.0 SIOP requirements

To explore the semantic interoperability issues arising from a typical Governance 2.0 network, we focus on the interactions between the following network entities:

1. Government customers – citizens, businesses and others;
2. Government systems and their personnel – front- and back-office applications as well as government officers (human agents) interacting with external information from other network entities;
3. Social media applications and sites – all forms of web 2.0 platforms including social networking, micro-blogging sites, wikis, Really Simple Syndication (RSS) feeds, mashups services and others; and
4. Third-party service providers – intermediaries, non-governmental organizations and private organizations providing specific services to the network.

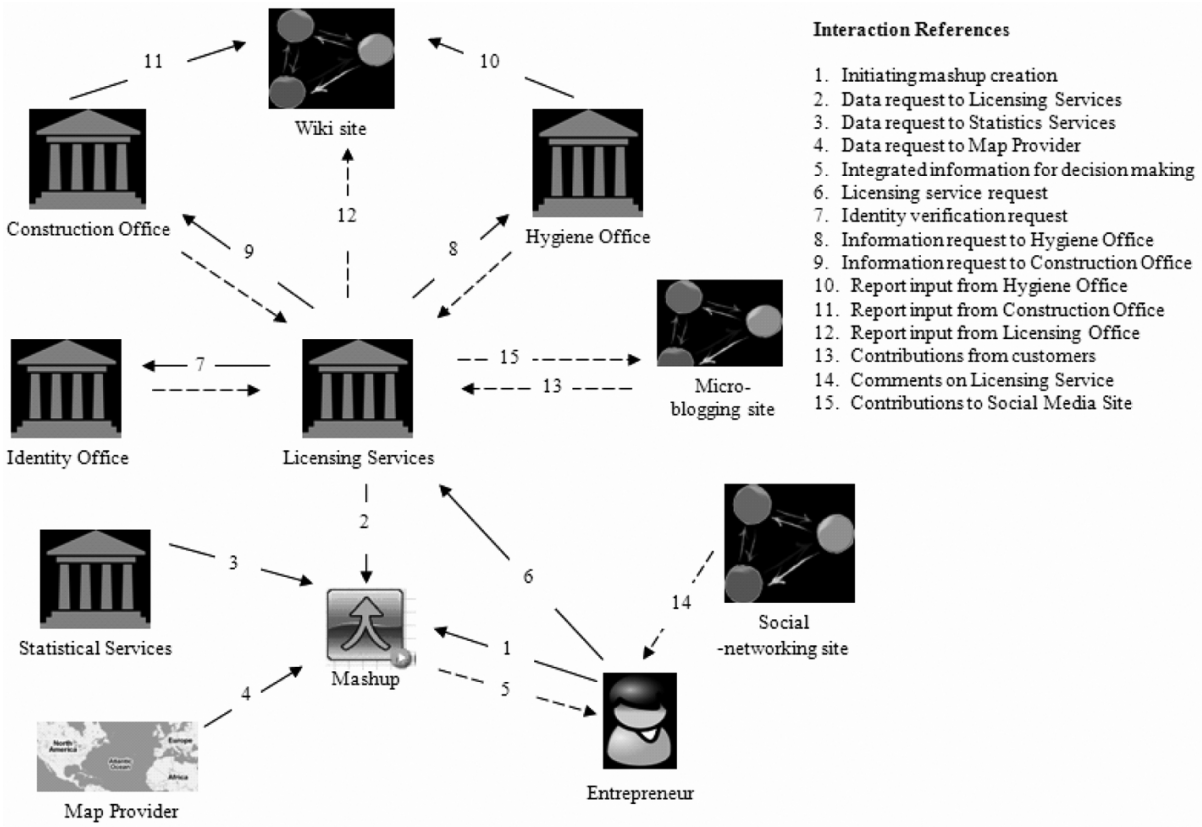

Fig. 4. Key interactions among major entities from case study.

Figure 4 illustrates the interactions among these entities in the context of the case study in Section 4.1.1. From these interactions, we can identify five important scenarios that raise significant semantic interoperability issues:

1. building mashups based on data sources from different government agencies;
2. broadcasting information to different social media sites through government feeds;
3. harvesting and aggregating social media contributions provided through different sites;
4. contributing contents to social media sites and consumption of contents on these sites by human agents; and
5. integrating information from different agencies at the back office.

Semantic issues arising from these scenarios are discussed below.

4.1.3. Scenario analysis

Scenario 1 – Building mashups from heterogeneous data sources

Data integration through mashup applications for decision support and gaining better insights to issues is becoming a primary aspect of service delivery and engagement-oriented interactions. For instance, in the case study, the entrepreneur requires the integration of spatially-referenced data from two agencies and mapping data from a third-party entity to decide on the location of his business. This scenario covers interactions 1 2, 3, 4 and 5 in Fig. 4.

The integration of data from diverse sources in a semantically-sound manner potentially presents a whole spectrum of semantic data integration issues. However, unlike in an enterprise where agreements and data integration are carried out over time between network members, data integration in mashup applications is done on demand. This implies the need for major standardization (and compliance) efforts affecting semantic descriptions of data provided by government agencies. Since the data is delivered as web services, available data services must be semantically described to minimize inaccurate retrieval. From the infrastructure perspective, the environments for building mashup applications must also support semantic information processing through access to semantic web APIs.

Scenario 2 – Broadcasting or publishing information to social media sites

Pushing government information into social media sites through government feeds is one of the most common uses of web 2.0 technologies in government. An example is the use of micro-blogging sites (e.g. Twitter) for publishing news and developments on state licensing services. This scenario is related to the interaction 15 in Fig. 4.

Feeding social media sites with contents directly from government systems raises a number of semantic issues. The first is to ensure that automatic update services provided by these sites are described with semantic information, to be discoverable by government systems. The second is to ensure that the site content models are understood by government applications for correct updates. The contents providers must ensure that the content is understood by the target audience in terms of the language used and its meaning.

Scenario 3 – Harvesting and aggregating social media contributions from different sites

The ability to access and integrate contents contributed by users in the form of opinions, feedback, ratings or general comments is to harness the collective intelligence of citizens in decision-making and obtaining valuable inputs for improvements in government. This scenario is related to the interaction 13 in Fig. 4.

Retrieving the contents that matches government needs (e.g. comments by businesses on a new licensing policy) or minimizing noise in retrieved contents is the first issue. Next, an aggregator service must ensure that the contents are meaningfully merged. For instance, the demographic analysis of public comments may cluster them into gender, education, age, etc. groups. In addition, the aggregator's ability to successfully merge contents from different sites assumes compatible content models, or requires the content mapping capability.

Scenario 4 – Contents contribution and access to social media sites by human agents

Human agents – officials, citizens and their representatives can contribute contents and tags, provide rating and review contents, and read the contents on social media sites [3]. For instance, in Fig. 4 the entrepreneur in interaction 15 is interested in reading comments about licensing services from others.

Semantic issues arising in this scenario include ensuring the understanding by human agents of the contents provided in the media in terms of their language, vocabularies and tags. In order to successfully exploit information from different sources, human agents must be able to map content elements from one social media to another in a semantically correct manner.

Scenario 5 – Integration of information from different agencies at the back office

Semantic back-office data integration in the agencies supporting cross-organizational processes raises the traditional semantic interoperability challenges. For instance, the license service request in Fig. 4 triggers through interaction 6 the back-office information exchange depicted by the interactions 7–9.

Using semantic differences catalogue [11] we identify in Table 1 the semantic issues for typical licensing services.

Table 1
Semantic issues arising from typical application evaluation activities

Step	Action	Semantic issue
Evaluation	– Providing technical opinion on information within government agency – Evaluating information by a third party – Requesting actions to third parties	The semantic differences could arise when: (i) supplying information to third-party organization, (ii) interpreting the outputs from the evaluation and (iii) evaluating the security context for the type of evaluation sought.
Decision	– Consolidating external inputs – Documenting decision – Communicating decision – Seeking additional input	Most of the semantic differences here will be associated with the consolidation of facts from different sources. In addition, semantic issues may also arise when requesting for clarification or more information from the customer.
Propagation	– Updating third-party agencies with application results	The semantic differences in this context relate to the anticipated effect of the update made to other agencies.

4.1.4. Summary

The above scenarios give rise to the following semantic issues:

1. Semantic data mediation service is required on demand and on the fly;
2. Data services provided by governments and third parties should be discoverable based on semantic descriptions;
3. The mashup development environment is required to support semantic information processing;
4. The services provided by social media sites should be discoverable by government systems and requested by them in a semantically valid manner;
5. Content models for social media sites should be understandable by government systems;
6. Government systems should understand the tags associated with social media contributions;
7. The contents contributed by agencies on social media must be understandable to target audiences;
8. Government systems should be able to aggregate contents in a semantically correct manner, identifying related information in particular;
9. Government systems must be able to map content models for social media sites;
10. Government systems must be able to map tags from different social media sites;
11. Government must make sure that published content is understandable to citizens in terms of the language and its meaning; and
12. Government systems must be able to mediate semantic differences arising from information exchange with other systems within and outside the government network.

Next, we present concrete semantic interoperability requirements related to the identified issues.

4.2. Requirements

This section presents SIOP requirements which cover the semantic scenarios in Section 4.1. These requirements are organized under the three SIOP capability types as explained in Section 3.1.

1. *Policy and Governance* – fulfilling these requirements establishes a strategic framework for developing semantic interoperability capabilities within a Governance 2.0 network to cover issues related to guiding principles underpinning semantic interoperability, roles and responsibilities of participants, and compliance to regulations.

2. *Organizational* – the requirements related to cooperation processes, enlisting participation of government organizations, evolution of communities and social networks, adoption of common business vocabularies and standards across government, and the use of controlled vocabularies for communicating with stakeholders.
3. *Technical* – technological capabilities that communities and network members should possess, for instance the availability of semantic descriptions of relevant enterprise assets, and availability of semantic gateways to resolve semantic differences in communication between COIs, and across social network sites.

4.2.1. Policy and governance requirements

We define five requirements in this category:

1. *Guiding Principles* – Clear principles and strategic drivers underpinning semantic interoperability within government and between government and its stakeholders is critical for developing semantic interoperability capabilities. For instance, supporting seamless service delivery, emergency management, citizen feedback on government policies, and access improvement to government through social media.
2. *Legal Frameworks* – Major legal issues constraining semantic interoperability – accessibility, authentication, authorization, security, transparency, accountability and privacy, should be clearly specified to guide SIOP solutions. This implies that related roles must be conversant with legal obligations related to data sharing and other cooperation initiatives, and subject to compliance review. In addition, specific conditions governing the production and use of contents on social media must be defined and understood by government agencies (Interaction 11 in Fig. 4).
3. *Roles and Responsibilities* – Identify important roles in major collaboration and data sharing initiatives and indicate specific responsibilities for them. For instance, different roles are required for clearing processes (clearinghouse) and audit processes in compliance review. However, on social media, governments can both create contents and exploit contributions as shown in Section 4.1. In addition, governments should participate in semantic standardization efforts e.g. on semantic interoperability and data portability for social media [28].
4. *Stewardship* – Clear identification of lead entities and ownership structures for information and semantic assets is critical for authority and necessary for successful semantic interoperability. The integrity, availability, publishing and updates of these assets will be guaranteed by their owners. However, ownership with respect to contents on social networks largely resides with their creators.
5. *Compliance Strategy* – A strategy to ensure that participating organizations comply with stipulated processes and discharge legal obligations. This could be developed along an incentives system.

4.2.2. Organizational requirements

Five requirements are specified in this category:

1. *Communities of Interest* (*COI*) – There is a need to define a process for creating communities of interest consisting of organizations with shared collaboration goals. COIs will describe their collaborations and create semantic assets to underpin exchanges involved in collaboration. The evolution and maintenance of shared semantic assets is undertaken by these communities and their participants. In addition, there is a need to identify groups on social networks of interest and their communication (language, vocabulary, etc.) needs.
2. *Information Context* – To ensure consistent use of shared data, there is a need to adopt a common business language for describing the context for the use of data assets. Therefore, a process for defining business taxonomies for the whole of government along functional lines is required.

3. *Semantic Asset Processes* – Processes for managing the lifecycle of semantic assets must be defined for the clearinghouse, along with standards and processes for creating and managing them.
4. *Collaboration Processes* – Processes must be developed to enable the provision of semantic support for collaborations between governments, intermediaries and suppliers, including social networks platforms, collaborative writing of reports on wiki platforms, etc. There is also a need to collaborate with third-party data providers for governments to provide mashup services [29].
5. *Training of Public Officers* – Specialized training is required for public officers contributing content and collecting data from social media sites.

4.2.3. Technical requirements

Eight requirements are cataloged in this section:

1. *Semantic Description* – Collaborating organizations should provide semantic descriptions, based on government-wide specifications and ontologies, of enterprise elements – shared data, collaborative processes, services and regulations, government and social networks, etc. as semantic assets – dictionaries, taxonomies, mapping tables, XML schemas, ontologies, etc. Government social networks should adhere to semantic interoperability standards for online communities related to open identity, collaborative tagging, semantic mashups, etc. [28,30]. This requirement covers Interaction 2.
2. *Local Semantic Asset Repository* – Providing storage and retrieval services for semantic assets at different organizations and collaboration parties as Local Semantic Asset Repositories.
3. *Local Metadata Registry* – Providing a Local Metadata Registry for publishing and managing the lifecycle of semantic assets by collaborating entities, able to push the updates to the Clearinghouse.
4. *Central Semantic Asset Repository* – Establishing a repository of semantic assets at the community or whole-of-government level as Central Semantic Asset Repository.
5. *Clearinghouse* – Developing a central metadata registry to manage the lifecycle of semantic assets on the Central Semantic Asset Repository, providing search and retrieval capabilities for semantic assets in the central repository as well as local repositories managed by individual organizations.
6. *Semantic Discovery* – Collaborating entities should be able to search the central metadata registry for required data, services and other resource types through the clearinghouse. Government systems should also be able to discover content services provided by social media sites (see Interaction 4).
7. *Semantic Gateway*: To enable semantic translation (mediation) of information between collaborating parties, there is a need to provide semantic gateway services. Relying on semantic assets provided through the Clearinghouse to resolve semantic differences, the Gateway must be able to validate data with respect to semantic assets and mediate semantic conflicts arising in different information exchange scenarios [11]. In addition, the Gateway should be able to mediate between government ontologies, social media contents from different sites, and map tags on social networks to government ontologies. This requirement implements semantic issues Interactions 1, 5, 6, 7, 9, 10 and 12.
8. *Interfacing with Collaboration Platforms*: The Semantic Gateway, Clearinghouse and other infrastructural elements would be required to interface with collaboration platforms, e.g. messaging gateways, workflows and mashup development platforms. This requirement covers I3 and I8.

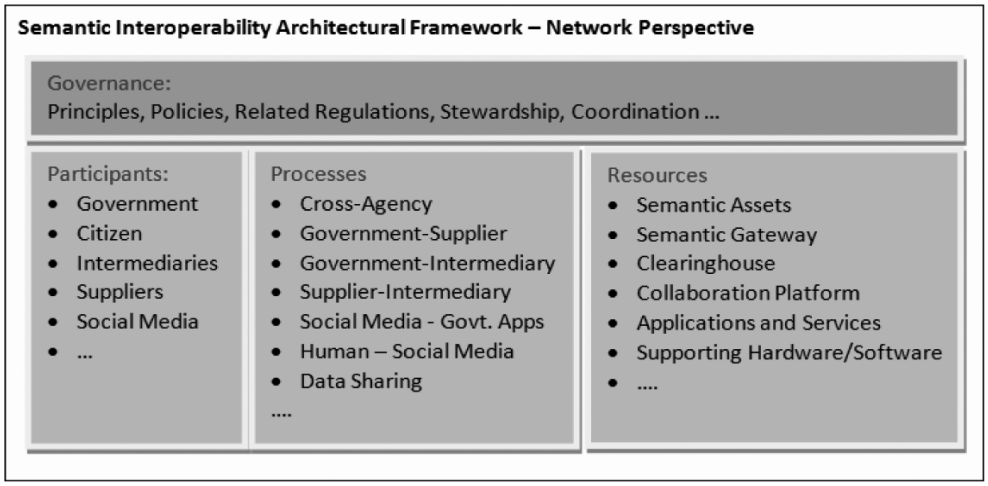

Fig. 5. SIAF – Network SIAF viewpoints.

4.2.4. Summary

The above requirements specify detailed capabilities for developing a comprehensive semantic interoperability solution for Governance 2.0. To guide the implementation of these requirements, we present reference architectures to associate such capabilities with specific architectural concerns at the network and member levels using the architectural patterns described in Section 3.2.

5. Semantic interoperability architectural framework

This section presents two complementary architectural frameworks for organizing the SIOP capabilities into SIOP reference architectures for the whole-of-government (network) and participant levels. It also shows how these architectural frameworks can be integrated for practical use and presents arguments for their validation.

5.1. Network-level architecture elements

As discussed in Section 3.2, we organize the capabilities for developing and managing semantic interoperability at the whole-of-government (network) level into four domains (see Fig. 5):

1. *Governance* – principles guiding the development of semantic interoperability capabilities across the government and within specific organizations, including rules, regulations and contracts governing semantic interoperation. This dimension addresses the requirements R1, R2, R4 and R5.
2. *Participants* – identifies various entities – government, suppliers, intermediaries, data service providers, etc. involved in Governance 2.0 networks, and specifies their responsibilities. It addresses the requirement R3.
3. *Processes* – identifies collaborative processes that require semantic interoperability – government-supplier, government-intermediary, cross-agency, data-sharing, information consolidation for social media, and organizational support for semantic interoperation. This aspect addresses the requirements R6, R7, R8 and R9.

Table 2
Network dimensions versus requirements

No.	Dimension	Requirement
N1	Governance	R1 – Principles R2 – Legal Framework R4 – Stewardship R5 – Compliance Strategy
N2	Participants	R3 – Roles and Responsibilities
N3	Processes	R6 – Communities of Interest R7 – Information Context R8 – Semantic Asset Processes R9 – Collaboration Processes
N4	Resources	R11 – Semantic Description R14 – Central Semantic Asset Repository R15 – Clearinghouse R16 – Semantic Discovery R17 – Semantic Gateway R18 – Interface with Collaboration Platform

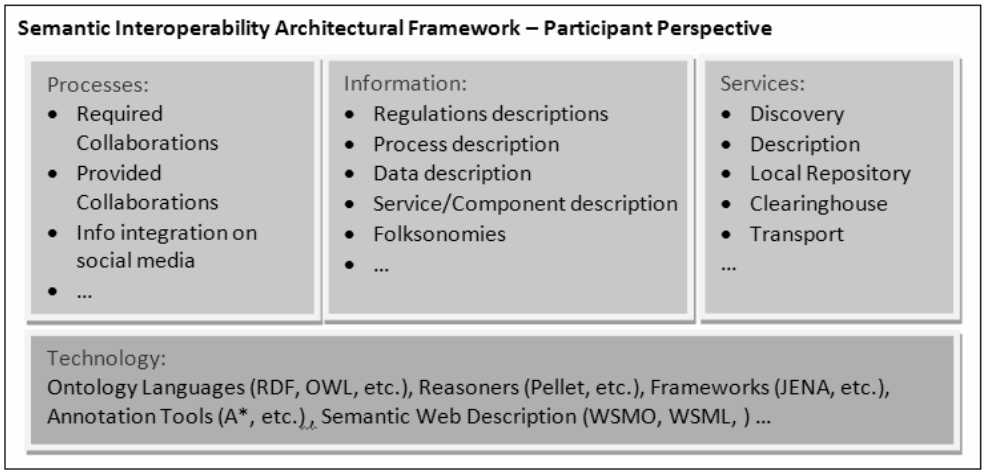

Fig. 6. Participant SIAF viewpoints.

4. *Resources* – information and technology resources required for implementing semantic interoperability, e.g. semantic assets for description and mapping, semantic gateway, clearinghouse, etc. Requirements R11 and R14 through R18 are addressed through this view.

Table 2 provides the mapping between network dimensions and semantic requirements addressed by them.

5.2. Participant-level architecture elements

The participant view of the reference model organizes the capabilities of each collaborating entity into Processes, Information, Services and Technology domains as shown in Fig. 7 and explained below:

1. *Processes* – Specifies the collaborations required by an agency or a third-party organization to fulfill its obligations as well as collaborations provided by the organization towards achieving

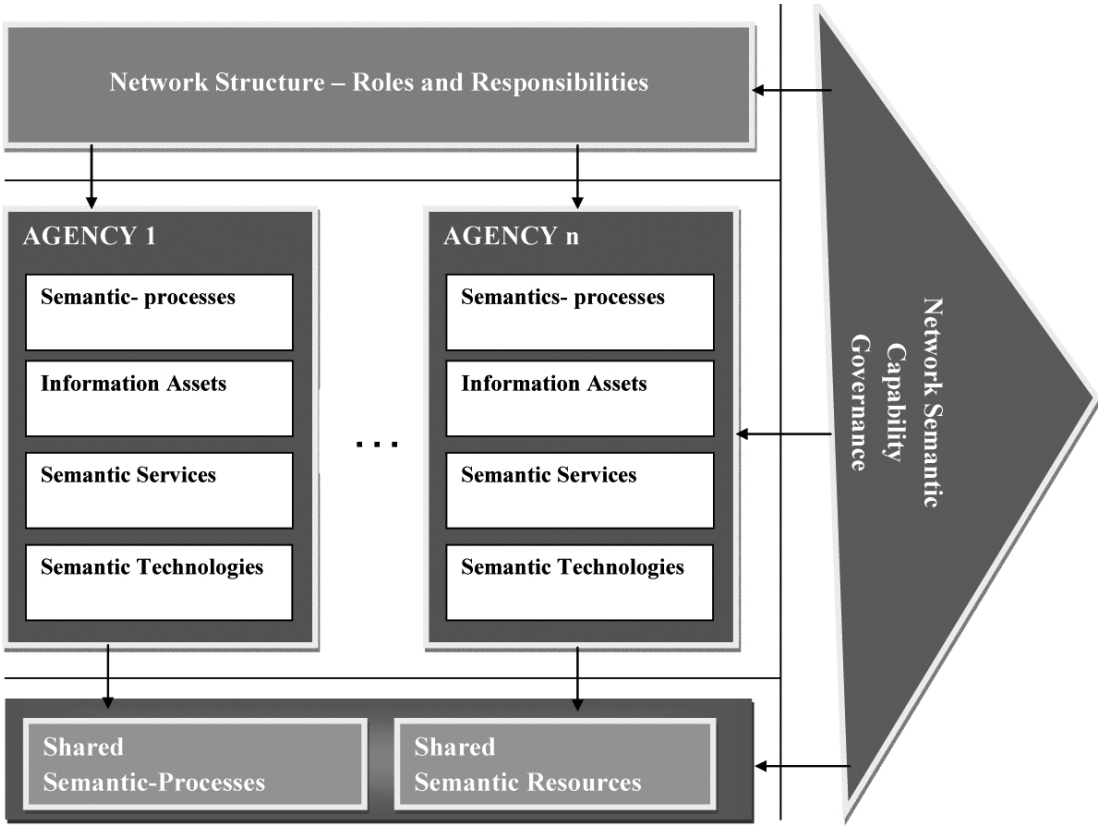

Fig. 7. Integrated semantic interoperability architecture.

government-wide, community-level or collective goals. This domain addresses the requirements R6 through R9.

2. *Information* – Specifies major semantic assets to be developed, including semantic descriptions of key aspects of the organization (data, processes, objectives, and regulations). This view captures the requirement R12.
3. *Services* – It includes applications, services and components to support semantic description, discovery and processing capabilities. This view addresses the requirements R11, R13, R16, R17 and R18. We assume that semantic mediation is handled centrally by the semantic gateway provided at the network level.
4. *Technology* – It specifies semantic technologies that organizations must acquire to develop semantic services, semantic assets and semantic-enabled processes.

Table 3 maps the viewpoints of the participant-level SIOP architecture to the associated semantic requirements.

5.3. Integrating network- and participant-level architecture frameworks

We explain how these two architecture frameworks can be integrated in practice to deliver whole-of-government or community-wide SIOP solutions. The network-level SIOP architecture provides the following services to network members: governance of SIOP activities, assignment of responsibilities

Table 3
Participant dimension versus requirements

No	Dimension	Requirement
P1	Processes	R6 – Communities of Interest R7 – Information Context R8 – Semantic Asset Processes R9 – Collaboration Processes
P2	Information	R12 – Local Semantic Asset Repository
P3	Services	R11 – Semantic Description R13 – Local Metadata Registry R16 – Semantic Discovery R17 – Semantic Gateway R18 – Collaboration Platforms Interface
P4	Technology	Supports the other three dimensions

to network members with respect to SIOP operations at the network level, and provision of network-level semantic infrastructure and resource-bases. Network members address their own semantic needs following the principle of subsidiary in terms of semantic-supported collaboration processes, semantic assets and services, and semantic technology acquisitions. This approach is consistent with the whole-of-government paradigm. Figure 7 illustrates an integrated SIOP architecture based on the two reference architectures. In this example, the agency architecture (depicted as Agency i) is a concrete instance of the participant-level SIOP architecture framework, while the Network Structure, Network Semantic Capability Governance, Shared Semantic Processes and Shared Semantic Resources are concrete instances of the Network-level SIOP architectural framework elements.

5.4. Validating the SIAF framework

We conclude this section by presenting arguments to validate the prescribed architectural frameworks for organizing the semantic interoperability capabilities articulated in Section 4. The premises for the validity of our architectural model with respect to the semantic interoperability requirements are as follows:

1. The two architectural frameworks are based on well-established architectural patterns: collaborative networked organizations [26] and enterprise architectures [27]. These architectural models provide standard viewpoints and well understood relationships.
2. By successfully mapping the cataloged requirements to specific viewpoints by the network- and participant-level frameworks, we demonstrated conceptually that the architecture satisfies the specified requirements.
3. By providing an integration model for both architectural frameworks in a manner consistent with the whole-of-government paradigm, we showed that the architectures can be implemented in practice.

6. Using the architecture framework

Our goal for SIAF is to guide the development of government semantic interoperability architectures – a holistic and multi-perspective approach to SIOP capability development, management and evolution. Therefore, a process to guide the development of concrete architectures is an important element of the framework. We highlight this process and provide concrete scenarios for the use of SIAF.

6.1. SIAF processes

At the network level, the critical steps in developing a concrete SIOP architecture from SIAF include: (i) defining the goals of the SIOP initiative and how success and benefits will be measured at the network and participant levels; (ii) identifying the stakeholders and participants involved; (iii) working out governance-related issues – eliminating barriers to cooperation, providing platforms to obtain semantic agreements, and providing a coordination machinery; and (iv) identifying the core inter-organizational processes and developing the semantic assets base for the network.

At the participant level, the following steps are necessary: (i) establishing SIAF readiness for each participating entity, (ii) prioritizing inter-organizational processes based on entity goals, and (iii) developing core semantic assets.

6.2. Other application scenarios

We identify three concrete use cases for SIAF:

- *Capability Assessment* – the framework could be used to develop instruments for measuring existing SIOP capabilities for networks and CIOs as well as readiness of network participants.
- *Roadmapping* – with prioritization scheme, the framework could be a basis for planning the development of SIOP capabilities in government.
- *Maturity Framework* – Given the possibility for detailed assessment instruments to be developed from SIAF, the framework could be combined with generic interoperability maturity framework [25] to assess the maturity of government semantic interoperability. For instance, the government SIF in Section 2 could be analyzed with respect to SIAF elements to indicate the level of completeness of these initiatives. However, in practice such evaluation will go beyond mere analysis of SIF specifications.

7. Conclusions

The goal of this article is to provide an architectural framework to assist government in developing Semantic Interoperability capabilities for their networks. The major contribution is analysis and articulation of the semantic interoperability requirements for Governance 2.0. In addition, we have shown how the semantic interoperability requirements (capabilities) can be organized into a whole-of-government architecture and how the architecture could be implemented in practice. Furthermore, we have attempted to bridge the knowledge gap in understanding the government semantic interoperability problem, since a consolidated view on the problem is yet to emerge.

Our observation is that few governments directly address semantic interoperability issues in their interoperability frameworks [31]. In addition, existing semantic interoperability frameworks do not address semantic issues associated with the use of Web 2.0 in government. This is not unexpected as Governance 2.0 has only gained momentum within the last five years. In fact, only a handful of governments (e.g. UK and US) have explicit strategies and initiatives for harnessing the benefits of social media in transforming service delivery and opening up governments. However, the increasing uptake of social media by governments and the need to better exploit their benefits is driving standardization particularly in social networks and data portability [28].

On the pragmatic aspect of the problem, we believe that semantic interoperability remains a complex and risky undertaking for governments as technological solutions are still immature, particularly for

Governance 2.0. To reduce the risk in the development of SIOP initiatives, we put forward the following recommendations:

1. SIOP should be conceived as a government "capability" to ensure a holistic approach to the problem as captured in SIAF. This implies that policy, organization and management issues such as strategic planning, project management and business case development [25] are critical for obtaining concrete SIOP benefits.
2. Although SIAF provides a comprehensive blueprint for SIOP initiatives, implementation must be staged and prioritized [24]. As the SIOP implementation depends on social, cultural and human factors within each participating organization and rests on the feasibility of the whole-of-government implementation, it is recommended that governments commence the SIOP initiatives modestly, with strong orientation towards learning, risk minimization and potentiality for benefits.
3. The development of semantic assets – ontologies, mapping tables, tags, ontology-folksonomy maps, etc. is difficult. A prudent mix of formal and social approaches is advised [32].
4. Governments should support and contribute to the emerging open standards for Web 2.0 in the areas of social networks, data interoperability and open identity management, to support their Governance 2.0 innovations.

Our future work includes further elaboration and formalization of the reference architectures, and the development of software tool support for government practitioners.

Acknowledgments

This work was carried as part of the Semantic Interoperability for E-Government (SIEG) Project. The authors would like to thank Microsoft Corporation for supporting the project.

References

[1] H.G. Frederickson and K.B. Smith, *The Public Administration Theory Primer*: Westview Press, 2003.
[2] J.E. Fountain, *Building the Virtual State: Information, Technology and Institutional Change*. Washington, D.C: Brookings, Institution Press, 2001.
[3] D. Osimo, Web 2.0 in Government: Why and How? Institute for Prospective Technological Studies, European Commission, JRC Scientific and Technical Report, 2008.
[4] A. Chang and P.K. Kannan, Leveraging Web 2.0 in Government, IBM Center for the Business of Government, E-Government/Technology Series 2008.
[5] F. Bettahar, C. Moulin and J.-P. Barthès, Towards a Semantic Interoperability in an e-Government Application, *Electronic Journal of e-Government* **7**(3) (2009), 209–226.
[6] K.K. Breitman, C. Howard Felicíssimo and L.M. Cysneiros, Semantic Interoperability by Aligning Ontologies, available at: http://wer.inf.puc-rio.br/WERpapers/artigos/artigos_WER03/karin_breitman.pdf.
[7] K.A. Stroetmann, G. Surjan, B. Ustun, M. Virtanen and P.E. Zanstra, Semantic Interoperability for Better Health and Safer Health Care, available at: http://ec.europa.eu/information_ society/activities/health/docs/publications/2009/2009semantic-health-report.pdf, January 2009.
[8] J. Rothenberg, M. Botterman and C. van Oranje-Nassau, Towards a Dutch Interoperability Framework – Recommendations to the Forum Standaardisatie, available at: http://www.rand.org/pubs/technical_reports/2008/RAND_TR552.pdf, 2008.
[9] J. Tschumperlin, Model-driven Semantic Interoperability using Open Standards: A Case Study, available at: ttp://www.d-m-s.co.nz/Model-driven_Semantic_Interoperability_V1.0.pdf, June 2007.
[10] Cabinet Office, e-Government Metadata Standard, e-Government Unit, Cabinet office, United Kingdom, Version 3.1, available at: http://www.govtalk.gov.uk/documents/eGMS%20version%203_1.pdf, August 2008.

[11] M. Billet, S. Bonomi, E. van der Graaf, E. Kirgiannakis, N. Loutas, A. van Overeem, V. Peristeras, K. Tarabanis and J. Witters, Business, Semantic and Technical Requirements for Semantic e-Government Services at National and Pan-European Level, SemanticGov, FP6-2004-IST-4-027517, available at: http://www. semantic-gov.org/index.php?name=UpDownload&req=getit&lid=311, 2006.
[12] M.A. Covington, Speech Acts, Electronic Commerce, and KQML, *Decision Support Systems* **22**(3) (1998), 203–211.
[13] J. Spendar, Speech Act Theory, Course notes, available at: http://odur.let.rug.nl/∼spenader/public_docs/speech_acts_groningen_NOV.pdf, 2004.
[14] M. Luck, P. McBurney, O. Shehory, S. Willmott and A. Link Community, Agent Technology – Computing as Interaction: A Roadmap for Agent Based Computing, 2005.
[15] S. Willmott, J. Dale and P. Charlton, Agent Communication Semantic for Open Environments: Issues and Challenges, available at: http://www.lsi.upc.es/∼steve/Publications/IC_TECH_REPORT_200240.pdf.
[16] S. Moca, A. Nasir, V. Overeem, V. Paristeras, R. Russo, K. Tarabanis, E. Triantafyllou, T. Vitvar, W. Waterfeld, K. Winkler and J. Witters, SemanticGov Project – Overall Conceptual Analysis – State of the Art Report, available at: http://www.enterprisearchitecture.info/Images/EIF/semanticgov _ITI_D012_Final_State-of-the-art_Report.pdf, January 2006.
[17] M. Schorlemmer and Y. Kalfoglou, Using Information Flow Theory to Enable Semantic Interoperability, University of Edinburg, available at: http://users.ecs.soton.ac.uk/yk1/ccia03.pdf.
[18] M. Schorlemmer and Y. Kalfoglou, On Semantic Interoperability and the Flow of Information, in: *ISWC'03 Workshop on Semantic Integration*, Sanibel Island, FL, USA, 2003, pp. 80–86.
[19] V. Peristeras and K. Tarabanis, Governance Enterprise Architecture (GEA): Domain Models for e-Governance, in: *Proceedings of the 6th International Conference on Electronic Commerce*, **60**, Delft, The Netherlands, 2004, pp. 471–479.
[20] G. Vetere and Lenzerini, Models for Semantic Interoperability in Service-Oriented Architectures, *IBM Systems Journal* **44** (October 2005), 887–903.
[21] R. Hodgson, I. Polokoff and D. Allenmang, FEA Reference Model Ontology (FEA-RMO), available at: http://osera.modeldriven.org/documents/FEARMO-ProjectReport.pdf, 2005.
[22] CIO Council, Office of the Management and Budget, FEA Program, Data Reference Model, available at: http://www.ocio.usda.gov/e_arch/doc/DRM_2_0_Final.pdf, 2005.
[23] IDABC, IDABC Contents Interoperability Strategy, Working Paper, IDABC European e-Government Services, available at: http://ec.europa.eu/idabc/servlets/Doc?id=24405, September 2005.
[24] Australian Government, Australian Government Information Interoperability Framework, Australian Government Information Management Office – AGIMO, available at: http://www.finance.gov.au, 2006.
[25] T.A. Pardo and G.B. Burke, Improving Government Interoperability: A Capability Framework for Government Managers, Center for Technology in Government, University at Albany, SUNY, 2008.
[26] L.M. Camarinha-Matos and H. Afsarmanesh, A Modeling Framework for Collaborative Networked Organizations", in *IFIP International Federation for Information Processing* **224** (2006), 3–14.
[27] A. Mulholland and A.L. Macaulay, Architecture and Integrated Architecture Framework, Capgemini, 2006.
[28] U. Bojars, A. Passant, J.G. Breslin and S. Decker, Social Network and Data Portability using Semantic Web Technologies, in *2nd Workshop on Social Aspects of the Web* (*SAW 2008*), BIS2008, 2008, pp. 5–19.
[29] J. Palfrey and U. Gasser, Mashup Interoperability and eInnovation, Berkman Center for Internet and Society, Harvard University, 2007.
[30] H.L. Kim, A. Passant, J.G. Breslin, S. Scerri and S. Decker, Review and Alignment of tag Ontologies for Semantically-Linked data in Collaborative Tagging Spaces, in: *2008 IEEE International Conference on Semantic Computing*, 2008, pp. 315–322.
[31] L. Guijarro, Semantic Interoperability in eGovernment Initiatives, *Comput Stand Interfaces* **31**(1) (January 2009), 174–180.
[32] R. Klischewski, Top Down or Bottom Up? How to Establish a Common Ground for Semantic Interoperability within e-Government Communities, in: *Proceedings of 1st International Workshop on E-Government*, Bologna, 2003, pp. 17–26.