



Collaboration for Human-Centric eGovernment Workflows

Khaled Gaaloul, François Charoy, Andreas Schaad, Hannah Lee

► **To cite this version:**

Khaled Gaaloul, François Charoy, Andreas Schaad, Hannah Lee. Collaboration for Human-Centric eGovernment Workflows. Governance, Risk and Compliance in Web Information Systems - Workshop in Conjunction with WISE2007, Dec 2007, Nancy, France. pp.195-206. inria-00182290

HAL Id: inria-00182290

<https://hal.inria.fr/inria-00182290>

Submitted on 25 Oct 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Collaboration for Human-Centric eGovernment Workflows

Khaled Gaaloul¹, François Charoy², Andreas Schaad¹, and Hannah Lee³

¹ SAP CEC Karlsruhe, Security & Trust Group
Vincenz-Priessnitz-Strasse 1, 76131 Karlsruhe, Germany

² LORIA - INRIA - CNRS - UMR 7503

BP 239, F-54506 Vandœuvre-lès-Nancy Cedex, France

³ University Hamburg Vogt-Koelln-Str. 30 D-22527 Hamburg, Germany
khaled.gaaloul@sap.com, charoy@loria.fr, andreas.schaad@sap.com,
lee@informatik.uni-hamburg.de

Abstract. The execution of cross-domain eGovernment processes is a challenging topic. In earlier work, we presented an approach based on collaborative workflows to support eGovernment interoperability. However, such collaborative workflows often appear to be lacking transparency and control supporting concepts and mechanisms. These are needed as eGovernment workflows appear to be heavily human-centric. What is in many cases described as collaboration appears to be a mere coordination and synchronization of processes, often ignoring human-centric interactions. One type of transparency and control supporting mechanism in human-centric collaboration is that of task delegation.

In this paper we aim to analyse the gap between coordination and collaboration in the context of workflow management for eGovernment. First, we present a real case study to identify the key distinguishing factors regarding collaboration as opposed to coordination. Based on this, we present our approach to support cross-organisational collaboration. In particular, we will focus on the concept of delegation in the context of heavily human-centric collaborative workflows. Finally, we propose a delegation extension and structured set of future requirements regarding a coordination architecture presented in earlier work.

Keywords: eGovernment, R4eGov, workflow coordination, workflow collaboration, delegation.

1 Introduction

Electronic government (eGovernment) is the civil and political conduct of government, including services provision, using information and communication technologies. The concept of eGovernment has been gaining ground from initial isolated to extensive research and applications. The prerequisites for an eGovernment enactment strategy are the achievement of a technological interoperability of platforms and a deeper cooperation and security at the organisational level. Those requirements are related with the environment in which the public agencies operate, strictly constrained by norms, regulations, and result-oriented

at the same time [1]. Actually, most governmental organisations offer electronic services within a collaborative environment. However, inter-organisational collaboration, especially by means of workflows, is not as widespread.

The R4eGov project consists of inter-organisational collaboration between European administrations [2]. An example domain for such collaboration is Europol⁴ (European Police Office) and Eurojust⁵ (European Judicial Cooperation Unit). It describes an interagency collaboration within the areas of law enforcement and justice. One of the objectives is to establish a collaboration, including information exchange between both parties based on legal constraints, such as European laws, to which they have to comply to, but sustain effective degrees of freedom for each department to solve their issues in the way they think is the most efficient and effective [3]. Those objectives can be achieved using collaborative workflows [4, 5]. This is a novel approach supporting interoperability between organisations without the burden of centralized workflow management systems. The perspective is to enable a particular workflow model to be executed collaboratively by different workflow engines located on the private network perimeters of their respective owners.

However, recent works [6, 7] presented new requirements such as control and transparency in collaborative workflows. What is in many cases described as collaboration appears to be coordination and synchronization of processes by ignoring human-centric interactions. Actually, we need to consider all the relevant participating systems and workflows even if they are not directly involved in the current control-flow sequence of the workflow.

This paper expands on earlier work we have done in R4eGov to support inter-organisational collaboration between European administrations based-workflow. We aim to elicit the collaborative requirements between Europol and Eurojust and the definition of methods and tools to support such an human-centric collaboration. This collaboration requires transparency and control supporting concepts and mechanisms. The concept of delegation had not yet been treated in sufficient detail in the context of heavily human-centric collaborative workflows, and is the subject of this paper to foster transparency and control mechanisms in collaborative workflows according to global policies and European law regulations in R4eGov.

The remainder of this paper is organized as follows. Section 2 presents a workflow example inspired from an R4eGov scenario and shows the difference between workflow coordination and collaboration. We motivate in section 3 the use of collaborative workflow management for eGovernment and present our approach to support cross-organisational collaboration. In particular, we will focus on the concept of delegation. Section 4 extends our approach and presents some future requirements. Section 5 presents some related work regarding delegation. Section 6 concludes and presents some future works.

⁴ <http://www.europol.eu.int/>

⁵ <http://www.eurojust.europa.eu/>

2 eGovernmental Workflow Scenario

We introduce in this section an R4eGov workflow scenario related to the European administrations collaboration. Europol and Eurojust are two key elements of the European system of international collaboration within the areas of law enforcement and justice. They carry out very specific tasks in the context of dialogues, mutual assistance, joint efforts and cooperation between the police, customs, immigration services and justice departments of the EU member states [3]. During their collaboration, Eurojust and Europol are involved and a number of legal instruments are used. A Specific scenario for this collaboration is the Mutual Legal Assistance (MLA)⁶.

2.1 Mutual Legal Assistance (MLA)

Figure 1 depicts a global workflow scenario called Mutual Legal Assistance (MLA) involving two national authorities of different European countries regarding the execution of measures for protection of a witness in a criminal proceeding. This simplified collaborative workflow is inspired by and in parts derived from the case studies delivered in the European research project R4eGov [3].

The workflow shows a member of the Europol National Unit in country A asking for an MLA request. The rules of procedure on the processing and protection of personal data at Eurojust refer to a "Case Management System" (CMS). The measure is to be executed in country B. Europol National Unit makes a written request of assistance (witness protection) to Eurojust National Member (EJNM) A. Then, EJNM A opens a Temporary Work File in the CMS, and contacts EJNM B forwarding the request of assistance. The EJNM B contacts the responsible national authority of country B. Finally, steps will be taken by the responsible national authority to provide the requested assistance.

As shown in the example, four different parties are involved in this collaboration. After the Europol National Unit A sends the request to the corresponding contact point it waits until the follow-up is established by the other authorities. What is going on between the two EJNMs A and B is not mediated to the Europol National Unit A. Hence, this appears to be more than coordination and synchronization of processes between governmental organisations. Actually, several of the depicted tasks involve human interactions and are possibly time consuming. For instance, steps taken by the responsible national authority to provide the requested assistance might involve several stakeholders that decide on this subject, hereby considering different aspects like the severeness of the case or concurrent investigations. With respect to transparency, the current process status needs to be communicated to EJNM B. In addition, unexpected events can happen during any task (unexpected in the sense that it cannot be modeled beforehand, e.g. changing bilateral agreements between countries A and B) that need to be propagated to every other participant of the collaborative

⁶ This case study has been performed in joint collaboration between Europol, Eurojust and Unisys in the context of the EU FP6 IST Integrated Project R4eGov.

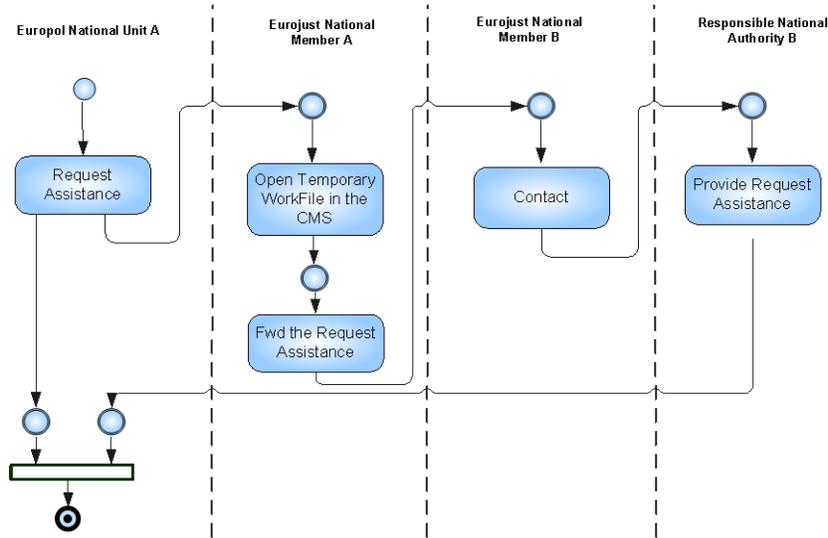


Fig. 1. Mutual Legal Assistance scenario

workflow (especially to the Europol National Unit A, the initiator of the collaborative workflow) even if they do not interact directly with each other in terms of control-flow.

2.2 Problem Statement

In the common understanding a collaborative workflow consists of one global workflow model composed of public views of each collaborative partner, with each public view abstracting a concrete private workflow behind it [5]. Existing choreography and collaboration approaches support the control-flow related message exchange that is part of the workflow model itself. Apparently this message exchange in case of status notification or cancellation is not part of the collaborative workflow model [6]. What is in many cases described as collaboration or collaborative mechanisms appears to be coordination and synchronization of processes by ignoring human-centric interactions. The requirements for interactions and monitoring can be summarized as transparency and control [8]. Transparency addresses the revelation of collaborative dependencies. This allows to react accordingly to exceptions and compensations implied by law regulations. Control fosters the behaviour of partners according to the collaborative policies (e.g. European laws).

This scenario depicts that we need to consider all the relevant participating systems and workflows even if they are not directly involved in the current control-flow sequence. Moreover, emergency situations can necessitate delegation of some activities intra and inter-organisations. For instance, EJNM B can

delegate its part of the work to the last party. This delegation has to be legal and compliant with the R4eGov laws regulations policies. In the next section, we motivate the concept of delegation as a support for transparency and control within an human-centric collaboration between Europol and Eurojust.

3 An Extended Analysis of Collaboration for eGovernmental Workflows

As stated before, control and transparency are important for a successful eGovernment collaboration. Hence, we follow a decentralized approach, combining the local workflows to form a collaborative workflow, integrating the existing systems of the involved partners, and adding a decentralized collaborative administration architecture to support human interactions (e.g. during a delegation request).

3.1 Workflow Engine Encapsulation

One re-occurring requirement is to enable collaborative workflows across different organisations without changes to the existing IT landscape of each organisation. A solution that enables collaborative workflows therefore needs to be built on top of existing solutions. Considering that assumption, the purpose of the workflow engine encapsulation is to offer a common interface to collaborative components (that would need to be deployed on each participants system) independent of the underlying workflow engine in place.

Such an interface needs to work in both directions: The collaborative components need to access engine and process specific functionalities. The process, during its execution, needs to publish events or performs requests to the collaborative components. Dealing with those requirements, we propose to set up a workflow to workflow collaboration by realizing a layer which we call an Administrative Communication Layer (ACL).

3.2 Administrative Communication Layer (ACL)

Wolter and *al.* [6] proposed an abstract modular infrastructure for collaborative workflow management and identified key components to leverage an existing workflow system onto decentralized collaboration. As indicated by Figure 2 the proposed architecture is divided into a control-flow layer and an administration layer.

In [7], we developed a prototype extended collaborative workflow tool to support the collaboration between the MLA partners. The term Administrative Communication Layer refers to the distinction of administrative events (e.g. starting/completion of one task) with control events (e.g. triggering a workflow instance) in each workflow engine. Our collaborative communication is event-based, on demand, or a combination of both. Therefore, ACL enables administrative information exchange by mediating information to the collaborative event management and process management components of the collaborative

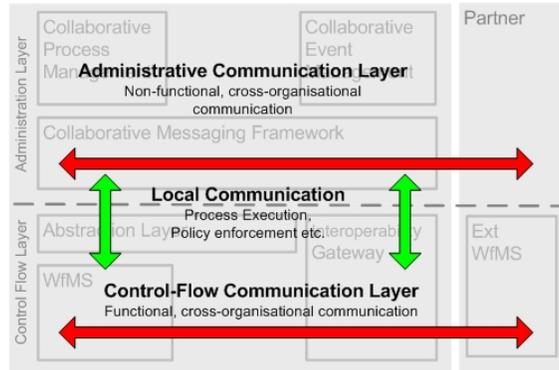


Fig. 2. Administrative Communication Layer

partners. The following aspects of administrative communication between the local process engine and the collaborative partners are supported:

- Status management to represent the overall status of the collaborative workflow (displaying the local process of the executing participant together with the overall workflow of all involved parties).
- Exceptions handling and execution of alternative scenarios which cannot be handled as part of the regular process model (e.g. EJNM delegates a part of his work to another authority due to legal changes).

3.3 Delegation Scenarios in MLA Request

Delegation is an important factor for secure distributed computing environments. It consists of delegating a part of a work to another partner according to laws regulations policies. Delegation can be motivated by many factors (e.g. lack of resources, organisational policies, etc.) [9] and can take place depending on the delegator/delegatee agreement. This agreement is closely related to the delegation criteria. In the following, we identify two different criteria of delegation from the MLA scenario:

Role-based delegation: The basic idea behind a role-based delegation is that users themselves may delegate role authorities to others to carry out some functions authorized to the former. Our interest is in the Eurojust’s side, the main actors involved in Eurojust’s information workflow are: Eurojust National Members and National Correspondents (NCs). Eurojust National Member of country A can play a role of a senior, an experienced prosecutor, or a judge. As a leader of the Eurojust organisation, EJNM, confronts problems that are particularly perplexing, collaborations are necessary for information sharing with members from the same organisation. Since EJNM believes in delegating responsibility,

he would like to delegate certain responsibilities to the NC member where the former define the delegation condition based on the organisation Role Hierarchy (RH) (see figure 3). The delegation request is inspired from RDM2000 proposed by Zhang and al. [10].

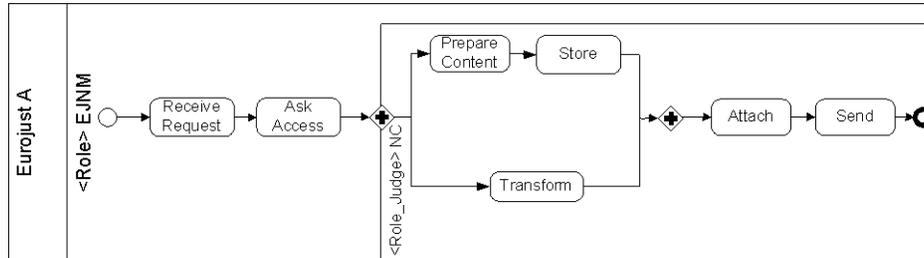


Fig. 3. Role-based delegation

Task-based delegation: Our interest is in the collaboration between the EJNM and the responsible of national authority in country B (see figure 1). What do we mean by task-based delegation is the delegation of a set of tasks to the delegatee. The condition of delegation depends on the organisational task alignment. Actually, a task T_i can be delegated if and only if the delegatee has a task T_j where T_j can give the same feedback/output than T_i and can substitute it. Due to emergency situations, EJNM B needs to delegate to an external party. The main task of EJNM B consists of determining the Judicial Authority (JA). Since the latter organisation role is JA, we assume that a delegation request can be motivated by the factor of specialisation. Nevertheless, the condition of delegation doesn't depend on the delegation factor (the specialisation of the JA member). Actually, a delegation request can be done if and only if the latter organisation offers the same service (set of tasks) to ensure the well and coherent deployment of the process. Coherency is closely related to the global policies of the MLA request. Here, our concern is the output of the task and not the "how" of the task. Since, the delegatee (JA member) provides tools, platforms and solutions to handle this delegation, there is no need to go deeper in his process attributes and then disclose his privacy. The agreement can be defined according to tasks alignment between organisations. This alignment is defined in the global policies of the process.

3.4 Extended Architecture

The scope of our approach is to address user-to-user delegation supporting human-centric collaborative workflows. We propose an abstract modular architecture to extend the architecture presented in [6].

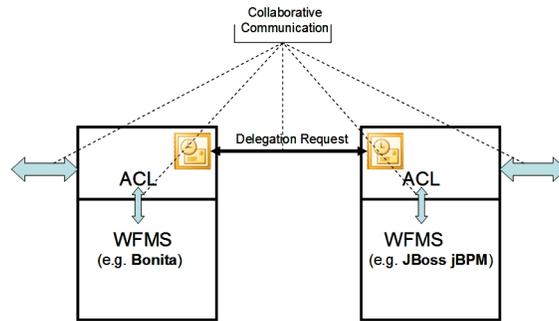


Fig. 4. Extended architecture supporting delegation

Once a delegator needs to delegate, ACL communicates a delegation request to the delegatee where the former invites the latter to accept to be in charge of one or more tasks of his local process.

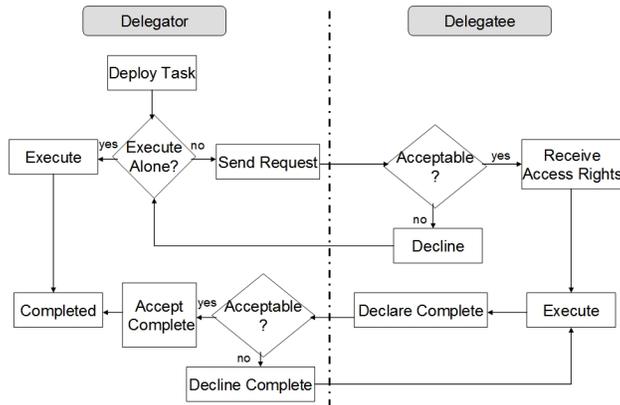


Fig. 5. Dialogue states and actions

A preliminary prototype implementation of the delegation mechanisms has been developed. It is based on mail request where a delegator sends a delegation request and wait for the approval of the receiver (the delegatee). The delegation dialogue between the two actors is depicted in figure 5. The acceptance/decline of the request and the delegating access rights (e.g. credentials, resources, etc.) will depend on the MLA global policies. Actually, "Receive Access Rights" step is more complicated: it depends on the delegation criteria (e.g. role, permission) and the availability of the resources to the delegatee. This step needs more investigations and time and will be a part of our future works.

4 Additional Requirements for Delegation

Delegation offers a suitable solution to support both ad-hoc and process-based interactions in an eGovernment context. In this highly dynamic environment, delegation is closely related to other concepts and mechanisms such as authorizations policies and revocation to allow the compliance and on-the-fly shift of responsibilities with respect to an ongoing collaboration both on a (atomic) task level and on a (global) process level.

4.1 Authorization Policy Model from the MLA Scenario

Authorization policy model can be used to specify public roles and their privileges and provides means to specify role mapping to internal and external roles of participating organisations. This specification will be used to identify the delegating access rights requirements afterwards. The Mutual Legal Assistance (MLA) scenario is being used as an example to illustrate the requirements of the authorization policy specification. Some of the related authorization policies rules are listed below:

1. **Europol National Unit A:** Only national units, liaison officers, and the Director, Deputy Directors or duly empowered Europol officials shall have the right to input data directly into the information system and retrieve it therefrom.
2. **Eurojust National Member A:** The case management system shall allow National Members to define the specific items of personal and non-personal data to which they wish to give access to other National Member(s), Assistant(s) or authorized staff members that are involved in the handling of the case.
3. **Eurojust National Member B:** When a National Member gives access to a temporary work file or a part of it to one or more involved National member(s), the case management system shall ensure that the concerned users have access to the relevant parts of the file but that they cannot modify the data introduced by the original author.
4. **Responsible National Authority B:** The case management system shall mark such data in a way that will remind the person who has introduced the data in the system of the obligation to keep these data for a limited period of time.

The involved participants are highly heterogeneous, and they intend to stay autonomous in terms of controlling their resources and executing tasks responsible for them. Moreover, fairly fixed, globally known roles for the collaboration are already established, and lastly, their privileges are often derived from European laws and regulations that must be followed by all participants. The last two characteristics make the Role Based Access Control (RBAC) model an extremely attractive choice to specify public roles and their privileges [11].

4.2 Revocation

Revocation is an important process that must accompany the delegation. It is the subsequent withdrawal of previously delegated objects such as a role or a task. A vast amount of different views on the topic can be found in literature [12, 13] where each author having their own assumptions and opinions on how to model revocation. For simplification, our model of revocation is closely related to the delegation model based user-to-user. Actually, the decision of revocation is issued from the delegator in order to take away the delegated privileges, or the desire to go back to the state before privileges were delegated. The privileges consist of the delegating access right provided to the delegatee. Basically, delegating access rights issued from the delegator describes the permission given to access to the task resources such as rogatory letters or legal requests in the MLA scenario.

5 Related Work

In this section, we present a literature review related to the delegation requirements. Basically, we aim to come up with a delegation classification of models, policies, and technologies that will fit with the motivation criteria for delegation in our future works.

The eXtensible Access Control Markup Language is an XML-based, declarative access control policy language that lets policy editors to specify the rules about who can do what and when. As an OASIS standard, its greatest strength lies in interoperability [14]. Unlike other application-specific, proprietary access-control mechanisms, this standard can be specified once and deployed beyond the boundaries of organisations and countries. In [15], Rissanen and Firozabadi add new structured data-types to express chains of delegation and constraints on delegation. The main result of their research is an administrative delegation. It is about creating new long-term access control policies by means of delegation in a decentralised organisation. However, this approach does not cover ad-hoc interactions and seems to not support decentralized delegation in the context of MLA.

In [16, 17], they tackle new requirements for delegation such as delegating in a dynamic and light-weight manner, performing single sign-on, and reusing existing protocols and software with minimal modifications. Welch and *al.* define *Proxy Certificates* allowing an entity holding a standard X.509 public key certificate to delegate some or all of its privileges to another entity. This delegation can be performed dynamically, without the assistance of a third party. However the problem with the X.509 proxy certificates is that commercial tooling for Web Services does not necessarily recognize and properly process these certificates [18]. Wang and Del Vecchio try to leverage and extend existing Web Services standards, without breaking the existing tooling by exploiting the Security Assertion Markup Language (SAML) inherent extensibility to create a delegation framework. They develop a set of verification rules for delegation tokens that rely on WSSecurity X.509 signatures, but do not force any trust relationship between the delegatee and the target service. However, this approach support

heavily computing and is time consuming that may slack the MLA deployment during a delegation request.

Role-based access control (RBAC) is recognized as an efficient access control model for large organisations. Most organisations have some business rules related to access control policy. Delegation of authority is among these rules [11]. In [19, 20], authors extend the RBAC96 model by defining some delegations rules. Barka and Sandhu proposed a role-based delegation model. They deal with user-to-user delegation. The unit of delegation in them is a role. However, users may want to delegate a piece of permission from a role [20]. Zhang and *al.* propose a flexible delegation model named Permission-based Delegation Model (PBDM). PBDM supports user-to-user and role-to-role delegations with features of multi-step delegation and multi-option revocation. It also supports both role and permission level delegation, which provides great flexibility in authority management. However, neither RBAC nor PBDM support the task-based delegation criteria described in the MLA delegation scenario.

6 Conclusion and Future Directions

In this paper we presented a novel approach to support an human centric collaborative workflow for eGovernment. Our primary concern is to analyse the gap between coordination and collaboration by distinguishing factors regarding collaboration as opposed to coordination. Actually, transparency and control supporting concepts and mechanisms are not taken into account in the context of heavily human-centric collaborative workflows. To satisfy this need we propose an extended architecture supporting task delegation as a mechanism in human-centric collaboration. Further, we discussed future requirements regarding a coordination architecture presented in earlier work.

We consider this paper as a primer for future related work in the areas of collaboration and security. Our concern will be to come up with a secure delegation mechanism supporting privacy and dynamic human interactions by addressing the delegating access rights issue. Moreover, we plan to further investigate the area of compliancy accordingly to the R4eGov laws regulations policies.

References

1. Roland Traunmüller, editor. *Electronic Government: Third International Conference, EGOV 2004, Zaragoza, Spain, August 30 - September 3, 2004, Proceedings*, volume 3183 of *Lecture Notes in Computer Science*. Springer, 2004.
2. R4eGov Technical Annex 1. Towards e-Administration in the large, March 2006. <http://www.r4egov.info>.
3. Eurojust / Europol collaboration, 2006. SIXTH FRAMEWORK PROGRAMME, Information Society Technologies, R4eGov.
4. Karsten A. Schulz and Maria E. Orłowska. Facilitating cross-organisational workflows with a workflow view approach. *Data Knowl. Eng.*, 51(1):109–147, 2004.

5. Mariangela Contenti, Massimo Mecella, Alessandro Termini, and Roberto Baldoni. A Distributed Architecture for Supporting e-Government Cooperative Processes. In *TCGOV*, pages 181–192, 2005.
6. Christian Wolter, Henrik Plate, and Cedric Herbert. Collaborative Workflow Management for eGovernment, September 2007. Accepted in the 1st international workshop on Enterprise Information Systems Engineering (WEISE).
7. S. Indrakanti, K. Gaaloul, M. Rahaman, and H. Plate. Prototype extended collaborative workflow tool, March 2007. Deliverable WP5-D3, SIXTH FRAMEWORK PROGRAMME, Information Society Technologies, R4eGov.
8. Chris Jensen and Walt Scacchi. Collaboration, Leadership, Control, and Conflict Negotiation in the NetBeans.org Community. In *26th International Software Engineering Conference*, 2004.
9. Vijayalakshmi Atluri and Janice Warner. Supporting conditional delegation in secure workflow management systems. In *SACMAT '05: Proceedings of the tenth ACM symposium on Access control models and technologies*, pages 49–58, New York, NY, USA, 2005. ACM Press.
10. Longhua Zhang, Gail-Joon Ahn, and Bei-Tseng Chu. A rule-based framework for role-based delegation and revocation. *ACM Trans. Inf. Syst. Secur.*, 6(3):404–441, 2003.
11. Andras Belokosztolszki, David M. Eyers, and Ken Moody. Policy Contexts: Controlling Information Flow in Parameterised RBAC. *policy*, 00:99, 2003.
12. Jacques Wainer, Akhil Kumar, and Paulo Barthelme. DW-RBAC: A formal security model of delegation and revocation in workflow systems. *Inf. Syst.*, 32(3):365–384, 2007.
13. Asa Hagstrom, Sushil Jajodia, Francesco Parisi-Presicce, and Duminda Wijesekera. Revocations-A Classification. In *CSFW '01: Proceedings of the 14th IEEE workshop on Computer Security Foundations*, page 44, Washington, DC, USA, 2001. IEEE Computer Society.
14. Ed. T. Moses. eXtensible Access Control Markup Language (XACML) Version 2.0, OASIS. Last viewed on Mar. 28, 2007.
15. Erik Rissanen and Babak Sadighi Firozabadi. Administrative Delegation in XACML. Swedish Institute of Computer Science, Kista-Sweden.
16. I. Kesselman C. Mulmo O. Pearlman L. Tuecke S. Gawor J. Meder S. Siebenlist Welch, V. Foster. X.509 Proxy Certificates for Dynamic Delegation, 2004. 3rd Annual PKI R&D Workshop.
17. Maarten Rits, Andreas Schaad, Stefano Crosta, and Jean-Christophe Pazzaglia. A Secure Public Sector Workflow Management System, December 2005. 21st Annual Computer Security Applications Conference, Tucson, Arizona.
18. Marty Humphrey and Jun Wang. Extending the Security Assertion Markup Language to Support Delegation for Web Services and Grid Services. In *IEEE International Conference on Web Services (ICWS 2005)*, volume 1. IEEE Computer Society, 2005.
19. E. Barka and R. Sandhu. Framework for role-based delegation models. In *ACSAC '00: Proceedings of the 16th Annual Computer Security Applications Conference*, page 168, Washington, DC, USA, 2000. IEEE Computer Society.
20. Xinwen Zhang, Sejong Oh, and Ravi Sandhu. PBDM: a flexible delegation model in RBAC. In *SACMAT '03: Proceedings of the eighth ACM symposium on Access control models and technologies*, pages 149–157, New York, NY, USA, 2003. ACM Press.