

Unraveling Decentralized Authorization for Multi-domain Collaborations

Hannah K. Lee
Security in Distributed Systems (SVS)
University Hamburg
Vogt-Koelln-Str. 30
D-22527 Hamburg, Germany
Email: lee@informatik.uni-hamburg.de

Abstract—Current authorization solutions take highly case-by-case approaches. First of all, the solutions address particular types of multi-domain collaborations such as Virtual Organization or resource-sharing collaborations. Secondly, they tend to be based on specific technology their subject interactions adopt. We consider this phenomena of having a number of different authorization solutions as a result of taking a mainly bottom-up approach to cater the authorization need of diverse types of multi-domain collaborations currently existing. In this paper, we present an extended analysis of different types of multi-domain collaborations based on various e-Government case studies as well as that of existing authorization solutions. With the converged requirements resulting from those analyses, we take a top-down approach of explicitly highlighting generic and interoperable components for a decentralized authorization scheme. This approach appears to be more suitable to produce a more efficient and elegant authorization solution for the majority of multi-domain collaborations.

I. INTRODUCTION

Are e-Government collaborations so different from e-Learning platforms or e-Business transactions? Are joint investigation teams of police officers so unique in their interactions that they require a different authorization framework from, for instance, hospital emergency collaborations? It is true that the e-Government collaborations do have specific criteria to satisfy, which are not so obvious in other types of application-level, multi-domain collaborations. A significant involvement of various levels of legislations and massive amount of sensitive data to protect can be a couple of distinct requirements of those collaborations. Nevertheless, speculating currently existing decentralized authorization solutions that are mainly formed for a specific technology or to cater particular scenarios-based specific collaborations [1], [2], one can not help questioning the existence of a generic set of requirements that can identify essential components for decentralized authorization at the application-level. This quest has been the motivation of the work presented in this paper.

Our analysis of current multi-domain collaborations show a couple of mainstream trends, either by enabling dynamic ad-hoc fashioned interactions or by forming a federated environment in which participants can collaborate. As far as decentralized authorization solutions are concerned, they address one or the other type of these collaborations as their target. Although these solutions state that their solutions can

be used for other type of collaborations, some functionalities and specifications will be unused or required to be modified if those solutions are to be deployed in other types of application scenarios.

Our findings from the e-Government scenarios of five different case studies tell no matter how diverse their use cases are, they boil down to a couple of generic interaction patterns, namely request/respond and publish/subscribe patterns. We also draw a proposition from comparing these case studies against the Organizational Interoperability Maturity Model C2 [3] that the application-level, multi-domain collaborations can easily be comprised of a mixture of ad-hoc or federated collaborations.

With the requirements that have been consolidated from the analyses of multi-domain collaborations and current authorization solutions, we propose three generic components for decentralized authorization. Although our analyses have only dealt with a subset of decentralized authorization solutions, this work can be a valuable starting point for developing a more refined and generic solution for decentralized authorization problems.

The rest of the paper is structured as follows. Section II describes five different e-Government collaboration case studies and draws commonly encountered characteristics of application-level, multi-domain collaborations. Section III discusses the current main-stream authorization solutions and elicits the converging requirements for authorization solution from the analyses discussed in Section II. Section IV presents three components for decentralized authorization solution based on the decentralized authorization requirement gathered. Section V states related work followed by the conclusion and the direction of the future work in Section VI.

II. ANALYSIS OF MULTI-DOMAIN COLLABORATIONS

Currently, there are two major trends in terms of forming multi-domain collaborations. One of them runs the collaboration in an *ad-hoc* fashion in a loosely coupled multi-domain environment whereas the other method is by creating a *federated* environment, which is designed to simulate a similar environment to a single domain. The former type of collaborations is commonly composed out of a group of peer-to-peer based bilateral collaborations. It is often hard to set up

a static path of execution, and collaboration partners may or may not have pre-established trust relationships. The common aims of such collaborations can be for incidental resource sharing or a single-step information exchange. By establishing a Service Level Agreement (SLA) or through an instance-based negotiation process, rules to interact are determined between collaboration partners before their interactions begin.

The latter approach is to create an artificial environment, which is more secure and enables even a centralized authorization service if desired. Their collaborations often include an established mechanism of building trust relationships amongst collaborative partners. In order to form a highly federated environment, they may need to employ the similar infrastructures, middleware, and proprietary specifications amongst collaborative partners. Some of the examples of the latter type are Virtual Organization and workflow management systems.

In the following subsections, we present the overview of five different e-Government case studies and the common characteristics of their collaborations.

A. Diagnosis of e-Government Collaborations

Five case studies provided by Boujraf et al. show various e-Government scenarios that encompass both ad-hoc and federated types of multi-domain collaborations [4]. The list below summarizes the key observations of the collaborations captured from each of the case studies:

- **German Supreme Court (Bundesgerichtshof – BGH)**

The BGH is a court of appeal aiming to safeguard legal conformity through the clarification and the development of law. Due to the highly specialized tasks that the BGH deals with, the number of actors involved in their collaborations are restricted to specific judges, lawyers and judicial clerks. Currently, their collaborations are mainly paper-based and within the organization [4].

- **Europol/Eurojust**

Europol, the European Police Office (EP) and Eurojust, the European Judicial Cooperation (EJ), are European agencies that have been set up to facilitate the 27 EU member states in their fight against cross-border organized crimes. To accomplish their primary mission, both Europol and Eurojust carry out distinct tasks in the context of joint efforts amongst the police, customs, immigration services, and justice departments of the EU member states [4]. Acquiring an European arrest warrant and requesting for a mutual legal assistance for witness protection during court proceedings are a couple of exemplary tasks of their collaborations.

In the collaborations of Europol and Eurojust with the EU member states, a number of globally visible roles have been detected. Their overall relationships are depicted in Figure 1, and the external roles are listed as following: Europol's Liaison Officers (ELOs), Member States' Liaison Bureaux (MS LBx), Europol National Units (ENUs), Member States' Law Enforcement

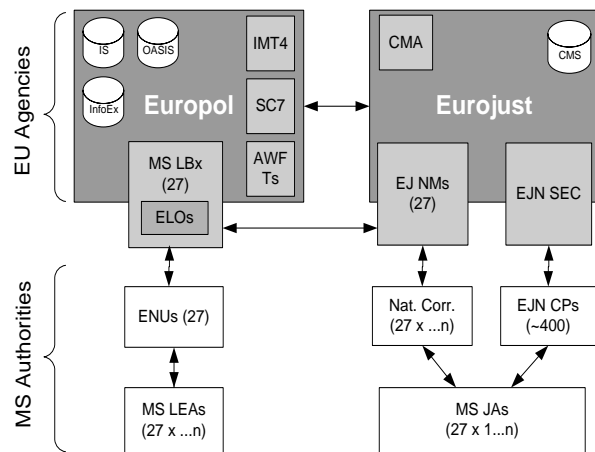


Fig. 1. Generic Overview of Europol & Eurojust Collaborations [4]

Authorities (MS LEAs), Eurojust National Members (EJ NMs), National Correspondents, Member States' Judicial Authorities (MS JAs), European Judicial Network Secretariat (EJN SEC), and European Judicial Network Contact Points (EJN CPs). Through these roles, approximately 5,000 users from the law enforcement side (involving 250-300 Law Enforcement Agencies with 17-20 officials each) and 750 users from the judicial side (involving 400 EJN Contact Points, the 27 National Correspondents on terrorism, the 27 Eurojust National Members, and additional 10 users per Member State) are involved in the Europol and Eurojust collaborations [4].

- **eVisa**

The eVISA case study focuses on the possible collaborations between the education institutes and the mobility facilitating agents (e.g. local consulates and border management posts) in order to deal with visa related issues of international students in the EU member states [4]. Numerous collaborative scenarios can be dynamically composed not only between public administrators for the purposes of border control but also between administrators and end-users for offering services to involved citizens. The eVisa case study also has the potential to include a larger number of countries due to the wide-spread student exchange programs among the universities within the EU member states as well as non-European country nationals studying in Europe [4].

- **Austrian Federal Chancellery (Bundeskanzleramt – BKA)**

Aiming to render the entire life cycle of legal texts in completely electronic format, the Austrian Federal Government has launched the e-Recht (e-Law) project in 2001 [4]. This case study illustrates various activities that can happen to the digitized legal text such as authoring, querying, reviewing, and transferring. Its main concern is between administration to administration

TABLE I
ANALYSIS OF E-GOVERNMENT CASE STUDIES

Use Cases	Readiness	# of Collaborators [4]	# of Potential Users [4]	Types of Collaborations	Maturity Level of Interoperability
BGH	X	1	≈ 440	N/A	Independent (0)
EP/EJ	V+	29	≈ 6000	Ad-hoc	Ad-hoc or Collaborative (1/2)
eVisa	X	World	≈ 3 million	Ad-hoc	Ad-hoc (1)
BKA	V+	5 (EU)	4-8 million	Federated	Collaborative (2)
eProcurement	V	27	136,000	Federated	Ad-hoc or Collaborative (1/2)

collaborations. Due to the lack of compatibility, only five other EU countries can interact with the current content repository addressed in this case study, but theoretically, its information system can be of use at the EU level once the interoperability issues are consolidated [4].

• eProcurement

The eProcurement case study deals with a cross-border call for tender process in the EU member states. A company which wishes to bid a cross-border call for tender in the EU is required to provide its legal existence and conform its national legal, fiscal, and social obligations [4]. On the other hand, a public authority receiving the tender must be able to check the validity of the submitted documents from the bidders. This verification task is handled by a third party authority called Trade Registers [4]. This case study has examined the particular scenarios related to Trade Register of the Paris Business Court (GTCP). Due to the differences among the EU country laws and regulations related to the public tender procedures, call for tender procedures may differ from a country to a country even within the European Union.

Excluding the BGH case study, all of the scenarios depicted in the case studies contain a large number of the potential collaboration participants. The *# of Collaborators* and *# of Potential Users* columns of Table I show numeric estimations of the size of the potential multi-domain collaborations. The *Readiness* column states informal ratings of deployment readiness for electronic multi-domain collaborations. The BGH and eVisa case studies are rated as *not ready* (marked with 'X') due to the lack of necessary technical and legal frameworks. The eProcurement case study is rated as *partially ready* (marked with 'V') since it is still bound by the limitations from national regulations. The EP/EJ and BKA case studies are rated as *ready* (marked with 'V+'), for they have foundational IT infrastructures and the legal endorsements for their collaborations.

The column, *Types of Collaborations*, classifies the case study scenarios with either *Ad-hoc* or *Federated* according to the earlier discussion we had in the beginning of Section II. The BKA scenarios are mainly within their content management system environment, and the eProcurement scenarios consider interactions amongst a closed group of bidders and a Trade Register. Therefore, their collaborations are more likely

within a federated environment. In the EP/EJ and eVisa scenarios, actors may join or leave any given time of a collaboration, and the course of their collaborations is dynamically decided. However, it is arguable that the distinction between *Ad-hoc* and *Federated* collaborations is rather unclear. For instance, in the beginning of eProcurement scenarios when a call for tender is still open to public, the collaborations are based rather on peer-to-peer interactions.

The *Maturity Level of Interoperability* of Table I classifies each of the case studies according to the Organizational Interoperability Maturity Model C2 defined by Clark and Jones [3]. Because interoperability is one of the fundamental hurdles multi-domain collaborations need to overcome, this model has been employed to foster the analysis of the characteristics of such collaborations. Their model defines five levels of interoperability maturity; from the lowest level, they are called: *Independent (0)*, *Ad-hoc (1)*, *Collaborative (2)*, *Integrated (3)*, *Unified (4)* [3]. While the lowest level represents an isolated environment without interoperability and the highest level, a complete interoperation, the three levels in the middle show different maturity levels of interoperability. The *Ad-hoc* level is characterized with shared goals but with limited organizational framework with liaison officers as the main means of information exchange whereas the *Collaborative* level is characterized with a recognized framework to support interoperability together with allocated roles and responsibilities [3]. The framework of the *Integrated* level is more mature than that of the *Collaborative* level with "shared value systems and shared goals, a common understanding and a preparedness to interoperate" [3].

The BGH case study is solely run within a closed environment and thus classified as the lowest level while the others are classified as *Ad-Hoc*, *Collaborative* or a mixture of *Ad-Hoc* and *Collaborative (1/2)*. An important discovery here is that most of the scenarios introduced in this section possess characteristics of both ad-hoc and federated collaborations and that some of them are a composite of those two types of collaborations (e.g. eProcurement and EP/EJ scenarios). The different types of collaborations are in fact drawn from different types of technologies that have been deployed. Another noteworthy point is that multi-domain collaborations do not pursue the top-levels of the C2 model since they desire to stay as autonomous as possible in terms of making decisions and controlling their resources in the course of collaborations. In other words, interoperability maturity level of multi-domain collaborations will most likely remain as they are regardless

of technical development.

B. Converging Properties of Multi-domain Collaborations

Here we summarize the commonly identified characteristics of multi-domain collaborations as the following five items based on the in-depth discussion provided in the previous subsection:

Autonomy. Collaborative organizations are highly heterogeneous in terms of their IT infrastructures and organizational policies. Yet, they wish to stay autonomous in terms of controlling their resources and making authorization decisions.

Dynamic path of execution. All of the case studies show dynamic characteristics due to the unknown factors to decide on an execution path and undecided participants in advance. A path of execution includes numerous possibilities as a scenario unfolds, and many case studies do expect collaborative partners to join or leave in the middle of a collaboration.

Privacy. Information pertaining to an end-user must not be disclosed unnecessarily during the process of authorization and to different domain scope. Moreover, at some cases, owners of resources should have explicit control over their information [5].

Representative actors. Most of the case studies contain fairly static and globally known roles as contact points to collaboration participating organizations. For instance, the scenarios in the BKA case study have notions of actors, roles, and their privileges in terms of handling document-centric resources. The EP/EJ case study also displays numerous globally known roles that are derived from well-known positions such as Europol Liaison Officers or European Judicial Network Contact Points.

Influence of external regulations. All of the case studies above incorporate some sort of external laws and regulations that are known to all collaborative partners. For instance, the privileges of the representative actors are partially defined in the overarching laws and regulations in the collaborative scenarios.

While the first three attributes of the common characteristics of the e-Government collaborations make a decentralized authorization more favorable than a centralized approach, the other two attributes offer possible optimizations to decentralized authorization solutions.

III. ANALYSIS OF AUTHORIZATION SOLUTIONS

A cross-organizational authorization requires a set of knowledge to be shared amongst collaborative partners so that each partner can make an authorization decision for requests originated from outside of their domains. The set of knowledge

can be described in a form of rule-based specifications or a portion of it can be composed during the execution time and transferred to different collaborative partners as a form of credential. In this section, first we discuss a couple of mainstream trends of decentralized authorization solutions and how they incorporate the set of shared knowledge, followed by its main generic requirements.

Rule-based solutions specify authorization constraints and conditions as a set of rules (e.g. authorization policy) [6]. Role-based Access Control and various extensions of the model are predominate examples of this category [7], [8], [9], [2], [10]. An extended analysis of different policies involved in the e-Government case studies provided in [11] also indicates that authorization policies are one of the types of policies that are suitable to be shared amongst collaboration partners. The downside of rule-based solutions is that they tend to be static and cumbersome to administrate in a decentralized manner. Some of their implementations also have non-standard format of specifications. Nevertheless, they can efficiently describe globally known roles and their relationships, which produce a more lightweight solution than solely relying on credential-based authorization mechanisms.

Credential-based solutions utilize a form of digital certificates to provide necessary properties of the holders such as their identities and accreditations, certified by a mutually agreed entity such as a certification authority (CA) [6]. Some of the examples of this category are SPKI, X509 certificates, and attribute certificates [12], [13], [14]. Through these methods, autonomy of collaborative partners can be respected; however, an evaluation of the credentials tends to cause latency during the execution time and may require a third party CA for verification of certificates.

Considering the converging attributes of multi-domain collaborations and current trends of authorization solutions, we draw the following to be primary requirements of a decentralized authorization:

Locality of control. Local authorities must be able to determine authorization decisions according to their own criteria, and each collaborative partner must be able to control which parts of their policies to disclose to other collaborative partners.

Compatibility with standard based solutions. Use of open, standard-based modules ensures that a solution can be suitable for the majority of multi-domain collaboration scenarios of heterogeneous communities. It also aids in scalable deployment without introducing significant changes to existing IT systems.

Flexible choices of enforcement mechanisms. It is necessary that a decentralized authorization model is not bound to a particular access control mechanism but rather enforceable by as many different types of enforcement mechanisms as possible.

Assurance between authorization specifications and enforcement mechanisms. Instead of taking a solution heavily relying on either rule-based solutions or on credential-based solutions, it is important to identify what is to be defined in the specifications and what is to be supplied through enforcement mechanisms with consideration of how to ensure assurance property between them [15]. Thus, decentralized management entities of keeping the two aspects of authorization in sync becomes important.

IV. GENERIC COMPONENTS FOR DECENTRALIZED AUTHORIZATION

Based on the requirements of decentralized authorization identified and stated in the previous section, we draw three components that can be deployed to the majority of multi-domain collaborations. The first is a model of authorization policy, which allows locality of control. The second component is a standard-based authorization mechanism, which preserves privacy. Lastly, the third component is a decentralized mechanism of holding assurance property between authorization specification and enforcement mechanisms. The following sections explain these generic components one after another.

A. Authorization Policy with d-Role

Having identified representative actors from most of collaborative partners in the e-Government case studies, it is in fact reasonable to utilize the RBAC model despite that counter-arguments exist. For instance, Ao and Minsky argue that the RBAC causes to create temporary roles when applied for delegation and that it is inadequate to express highly dynamic policies [16]. Although their point is valid for certain applications, in multi-collaborative scope, we reason that roles should not be created for the sake of delegation but that delegation specification should be defined out of the roles known to collaborative partners. Preserving autonomy of collaborative partners, we narrow down what must be shared amongst collaborative partners as a set of roles known to all. Consequently, this allows each participating organization to be in charge of specifying access control constraints within its local policies. We reason that this design of separating authorization specifications from access control policies enables participating organizations to flexibly update and manage their own resources and corresponding access control policies. In addition to it, incorporating this piece of knowledge of representative actors can make the necessary decentralized authorization more efficient and lightweight. To do so, we have adopted the notion of *distributed role* from dRBAC. It provides another layer of abstraction between two different sets of roles from different organizational domains [17]. Through this indirection, roles can be mapped from public and private viewpoints of a participating organization without causing changes in a global realm.

Figure 2 illustrates an overview of how d-Role concept can bridge the organizational boundaries in multi-domain collaborations. In the figure, d-Role is further sub-classified

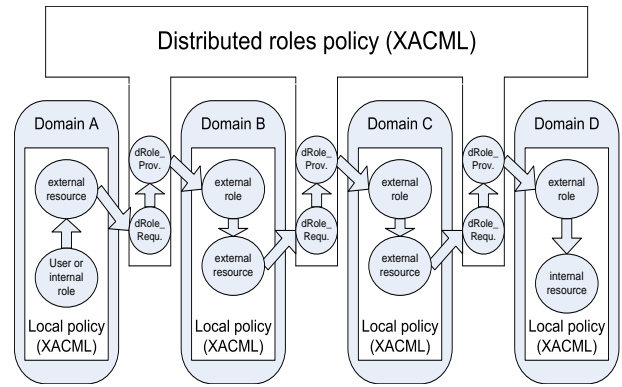


Fig. 2. Overview of Decentralized Authorization using d-Role

as *d-Role Provider* and *d-Role Requester*, providing further distinction between a requester and a provider. Lee and Luedemann motivate extending the eXtensible Access Control Markup Language (XACML) core specification to specify d-Roles and provides a viable implementation design in [18]. The set of privileges to a corresponding d-Role can be added as attribute fields of d-Role elements. The d-Role concept elegantly encapsulates the set of knowledge that needs to be shared among the collaborative partners.

B. Privacy-preserving Authorization Enforcement

The simple interaction patterns (e.g. request/response and publish/subscribe) identified in the case study scenarios ensure that authorization enforcement only needs to deal with bilateral interaction. So long as an authorization enforcement mechanism complies with standard-based solutions such as SAML [19], any enforcement mechanism should be able to be deployed depending on its suitability to a given collaboration. Nonetheless, some mechanisms are more suitable to provide necessary requirements such as preserving privacy. For instance, a subject field of an attribute-based certificate can be easily substituted from an internal role to a corresponding d-Role before the certificate is prepared to be sent out to a collaborative partner. From the recipient's point of view, a valid d-Role and a valid certificate certified by a trusted authority would be enough to process an authorization. Thus, sensitive information such as Personally Identifiable Information (PII) can be guarded from unnecessary disclosures. While specifications of which data should be treated as private can be incorporated within individual local policies, multi-domain authorization enforcement mechanisms should be capable of coping with various techniques to preserve privacy such as using pseudonym for disguising user identity.

C. Administrative Collaboration for Multi-domain Collaborations

Administrative collaborations are separate multi-domain collaborations, dedicated for specifying non-functional requirements for multi-domain collaborations. One of the examples of their activities can be defining d-Roles. In e-Government collaborations, d-Roles are drawn from glob-

V. RELATED WORK

As far as the methodologies of analyzing multi-domain collaborations in security perspective concerned, not so many choices are available. The one our requirement engineering team has deployed was the SQUARE methodology developed by Carnegie Mellon University [22]. It gives a general guideline of eliciting security requirements. Security and Dependability Tropos Tool is another possibility. Its highly sophisticated graphical interface offers to model various relationships amongst different roles, positions, and actors from different domains. Its functionality of expanding and hiding certain parts of the graphical components can be potentially beneficial for a privacy preserving purpose. It also provides formal analysis tools for the model developed from the GUI-based interface [23]. The drawback of Security and Dependability Tropos Tool is that it does not provide a translation from the requirement set to a set of rules that can be easily deployed to policy specifications.

As far as decentralized authorization for multi-domain collaborations is concerned, a wide range of solutions are available. Traditional trust management systems such as KeyNote [24] and SDSI/SPKI [12] can be used as a decentralized authorization service as well, but they need to be extended with credential discovery and revocation mechanisms. Role-based trust management (*RT*) combines the strengths of role-based access control and trust management systems and is capable of expressing attribute-based access control [25]. This is not the case with the traditional trust management systems. Using the mechanism of delegating authorization decisions to authorities in different domains, they not only provide trust establishment in a multi-domain setting, but some of them also enable a role activation procedure [17].

In addition to more flexible expressiveness of semantics, the advantages of *RT* over the previous trust management solutions include: a declarative, logic-based semantic language specification, strongly-typed credentials and policies, more flexible delegation structures, and more expressive support for separation of duty constraints [26]. While *RT* systems do offer variety of features for a decentralized access control, they require significant support infrastructures and extra installations for their framework to work properly.

dRBAC stands for distributed Role-based Access Control system, and it claims to provide a decentralized access control mechanism through a complete delegation solution that delegates roles to other roles or entities in another local name space where entities may refer to users or resources. Its infrastructure includes proof monitors, among others, which verifies delegation chains at each entity [17]. This model takes a similar approach to *RT* in the usage of a delegation chain for establishing trust and deferring authorization decisions. Ma and Woodhead have applied this model to resolve the problems of identity management inherent in a distributed subscription-based resource sharing environment [27]. This application of dRBAC for subscription-based resource providers does get its mileage out of the abstract layer of external roles as a number

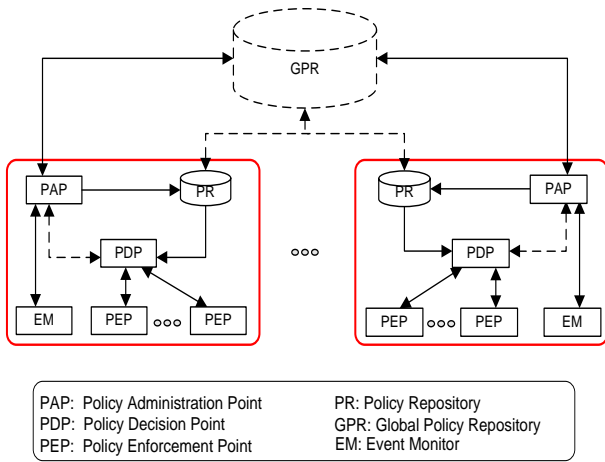


Fig. 3. Overview of Policy Administrators' Collaboration

ally known positions and their privileges according to the involved laws or regulations. In other cases however, they may be defined from different sources or mechanisms. The administrative collaborations may run in parallel to the actual collaborations they are administrating or they may run in advance to the subject collaborations. This component not only enables timely updates of globally known shared information, but it also provides necessary collaborative administrations for more flexible and dynamic courses of collaborations. It can be also used as a medium to foster assurance property between specification and mechanisms of multi-domain authorization solutions.

Figure 3 depicts a bird's eye view of how administrators from different domains may collaborate. Those two rectangular frames at the lower part of the diagram represent a conventional, single domain policy enforcement system, which is being widely adapted from the IETF/DMTF model to the XACML framework [20], [21]. Each of these frames is comprised with four components – Policy Repository (PR), which stores the policies of the organization, Policy Administration Point (PAP), which manages policy repository, Policy Decision Point (PDP), which evaluates the rules retrieved from the policy repository and makes an authorization decision, and Policy Enforcement Point (PEP), which sends a request to a PDP and executes the policy decision replied from a PDP. In the figure, a Global Policy Repository (GPR) is depicted with dotted lines. It represents a set of knowledge that is being shared amongst collaborative partners. It is conceptual and thus can be virtual in reality. For instance, in case of the authorization policy using d-Roles, it would be the list of d-Roles and their privilege descriptions. Through this framework, PAP's from different domains exchange necessary informations and store relevant portions of the conceptual GPR in their local policy repositories. The active interactions amongst PAP's from collaborative partners can coordinate different types of multi-domain collaborations, either ad-hoc or federated type.

of requesters per a given resource increases. Nevertheless, specifying distributed roles related entities, role constraints, and predicates in Distributed Role Markup Language (DRML), which they have developed, it requires cross-organizational specification to be written in their own language [26].

VI. CONCLUSIONS

In this paper, we have pinpointed the current trends of developing authorization solutions for restricted types of multi-domain collaborations. Critiquing this to be a result of using a bottom-up approach, we have shown a multiple number of e-Government collaboration scenarios and analyzed their interaction types and interoperability maturity levels to draw a more generic set of authorization requirements. We have also drawn authorization requirements from the diagnosis of current authorization solutions for multi-domain collaborations. As a result, we have identified a set of converging requirements of decentralized authorization. Our authorization solution captures those discovered converging requirements and aims to provide generic components that can be utilized by more broad range of multi-domain collaborations as reasoned in Section IV. We have provided a high-level overview of a three-fold solution with 1) an authorization policy using d-Role, 2) a privacy-preserving access control mechanism with attribute certificates, and 3) a collaborative administrative framework. This work contributes as an initiative of extracting generic components of decentralized authorization required for multi-domain collaborations. This would spur producing more efficient and effective solutions for the majority of multi-domain collaborations. We would also like to promote the need of a more systematic methodology of analyses on ever-increasing multi-domain collaborations and their inter-domain authorization solutions.

Currently, we are implementing the d-Role specification authoring tool according to the design explained in [18]. Our immediate future plan is to model an administrative collaboration framework as described in Section IV-C and enhance the policy authoring tool with the administrative collaboration functionalities with other collaborative partners.

ACKNOWLEDGMENT

The author would like to thank Christopher Alm and the anonymous referees for their valuable comments. The author would also like to thank the security requirement engineering team and the user group partners of R4eGov project for their contribution to the case study provisions and analysis.

This work has been funded by the EU Commission under the contract number IST-2004-026650 through the EU integrated project, Towards e-Administration in the Large (R4eGov).

REFERENCES

- [1] J. Jin and G.-J. Ahn, "Role-based Access Management for Ad-hoc Collaborative Sharing," *SACMAT '06: Proceedings of the eleventh ACM symposium on Access control models and technologies*, pp. 200–209, 2006.
- [2] Y. Demchenko, C. de Laat, L. Gommans, and R. van Buuren, "Domain Based Access Control Model for Distributed Collaborative Applications," *E-SCIENCE '06: Proceedings of the Second IEEE International Conference on e-Science and Grid Computing*, p. 24, 2006.
- [3] T. Clark and R. Jones, "Organisational Interoperability Maturity Model for C2," *1999 Command and Control Research and Technology Symposium*, 1999.
- [4] A. D. A. Boujraf and M. Noble, "Final Master Case Study of Collaborative Public Sector," *Towards e-Administration in the Large (R4eGov), Deliverable WP3-D7*, 2007.
- [5] "Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA)," http://eurojust.europa.eu/official_documents/Eurojust_Decision/L_06320020306en00010013.pdf, 2002 (Last viewed on 01.10.07).
- [6] S. D. C. di Vimercati, S. Foresti, S. Jajodia, and P. Samarati, *Ch2: Access Control Policies and Languages in Open Environments, Secure Data Management in Decentralized Systems*. Springer, 2007, pp. 21 – 58.
- [7] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.
- [8] J. S. Park, K. P. Costello, T. M. Neven, and J. A. Diosomito, "A Composite RBAC Approach for Large, Complex Organizations," *SACMAT '04: Proceedings of the ninth ACM symposium on Access control models and technologies*, pp. 163–172, 2004.
- [9] S. Ponomarev and J. B. D. Joshi, "An RBAC Framework for Time Constrained Secure Interoperation in Multi-domain Environment," *IEEE Workshop on Object-oriented Real-time Databases (WORDS-2005)*, 2005.
- [10] A. Belokosztolszki, D. M. Eysers, and K. Moody, "Policy Contexts: Controlling Information Flow in Parameterised RBAC," *Policy 2003: IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, pp. 99–110, 2003.
- [11] H. Lee, "Requirements for technical specification, enforcement and management of collaborative workflow security policies, including separation of duties and time constraint," *Towards e-Administration in the Large (R4eGov), Deliverable WP6-D2*, 2007.
- [12] C. Ellison, "RFC 2692: SPKI Requirements," September 1999. [Online]. Available: <http://www.ietf.org/rfc/rfc2692.txt>
- [13] R. Housley, W. Ford, W. Polk, and D. Solo, "RFC380: Internet X.509 Public Key Infrastructure: Certificate and CRL Profile," Apr. 2002. [Online]. Available: <http://tools.ietf.org/html/rfc3280> (Last viewed on 10/07/2007)
- [14] S. Farrell and R. Housley, "RFC 3281: An Internet Attribute Certificate Profile for Authorization," 2002.
- [15] S. Jajodia and T. Yu, *Ch.1: Basic Security Concepts, Secure Data Management in Decentralized Systems*. Springer, 2007, pp. 3 – 20.
- [16] X. Ao and N. H. Minsky, "On the role of roles: from role-based to role-sensitive access control," *Proceedings of the Ninth ACM Symposium on Access Control Models and Technologies*, Jun. 2004.
- [17] E. Freudenthal, T. Pesin, L. Port, E. Keenan, and V. Karamcheti, "dRBAC: Distributed Role-Based Access Control for Dynamic Coalition Environments," in *In Proceedings of the Twenty-second IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2002.
- [18] H. Lee and H. Luedemann, "A Lightweight Decentralized Authorization Model for Inter-domain Collaborations," in *Proc. ACM Workshop on Secure Web Services*, Nov. 2007 (to be appeared).
- [19] J. Hughes and E. Maler, "Security Assertion Markup Language (SAML) 2.0 Technical Overview," Feb. 2005. [Online]. Available: <http://xml.coverpages.org/SAML-TechOverview20v03-11511.pdf> (Last viewed on 10/07/2007)
- [20] B. Moore, "RFC3460: Policy Core Information Model (PCIM) Extensions," <http://rfc.net/rfc3460.html> (Last viewed on Mar. 28, 2007), 2003.
- [21] "eXtensible Access Control Markup Language (XACML) Version 2.0," Feb. 2005, (Last visited on 8/23/2007). [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf
- [22] N. R. Mead, "SQUARE Process." [Online]. Available: <https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/requirements/232.html> (Last viewed on 10/07/2007)
- [23] "Security and Dependability Tropos Tool." [Online]. Available: <http://sesa.dit.unin.it/sttool> (Last viewed on 10/07/07)
- [24] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The

KeyNote Trust-Management System Version 2," RFC 2704, 1999.
[Online]. Available: <http://www.ietf.org/rfc/rfc2704.txt>

[25] N. Li, J. C. Mitchell, and W. H. Winsborough, "Design of a Role-based Trust Management Framework," in *Proc. IEEE Symposium on Security and Privacy*, Oakland, May 2002.

[26] N. Li, J. C. Mitchell, W. H. Winsborough, K. E. Seamons, M. Halcrow, and J. Jacobson, "RTML: A Role-based Trust-management Markup Language," Purdue University, Tech. Rep., 2004.

[27] M. Ma and S. Woodhead, "Constraint-Enabled Distributed RBAC for Subscription-Based Remote Network Services," *CIT '06: Proceedings of the Sixth IEEE International Conference on Computer and Information Technology (CIT'06)*, 2006.