Identity Management for Virtual Organizations

A Survey of Implementations and Model

Robert Cowles, Craig Jackson, Von Welch
Center for Applied Cybersecurity Research
Indiana University
Bloomington, Indiana, USA
bob.cowles@gmail.com, scjackso@indiana.edu, vwelch@indiana.edu

***Abstract*—The Virtual Organization (VO) has emerged as a fundamental way of structuring modern scientific collaborations and has shaped the computing infrastructure that supports those collaborations. One key aspect of this infrastructure is identity management (IdM), and the emergence of VOs introduces challenges regarding how much of the IdM process should be delegated from the resource provider (RP) to the VO. Many different implementation choices have been made; we conducted semi-structured interviews with 14 different VOs or RPs regarding their IdM choices and the bases behind those decisions. We analyzed the interview results to extract common parameters and values, which we used to inform our VO IdM Model. This model will serve both existing and future VOs and RPs to more effectively understand and implement their IdM relationships. In this paper we present our VO IdM Model, the interview results that informed it, and preliminary analysis on the factors that guide VOs and RPs to choose a particular IdM implementation.**

Keywords—virtual organizations; identity management; security; collaboration; trust; risk

I. Introduction

The Virtual Organization (VO) has emerged as a fundamental way of structuring modern scientific collaborations and the computing infrastructure that supports those collaborations. One key aspect of this infrastructure is identity management (IdM), which has been extended to include the VO in the IdM process.

As we describe in subsequent sections, there have been numerous implementations of IdM extended to include the VO in different ways, but the community creating and choosing these implementations has no framework for describing these different choices nor an agreed-to methodology for when to choose one option over another.

Our goals are to provide both a common language for VOs and resource providers (RPs) to describe IdM implementations in the context of VOs, and provide guidance to those parties in making implementation choices to best meet their trust and risk requirements. Without these tools, VO IdM implementations are hampered due to complexity, a lack of overarching decision frameworks, and reduced clarity regarding the repercussions of decisions.

This paper takes a first steps towards achieving our goals and makes two contributions to IdM and Virtual Organizations: (1) we conducted semi-structured interviews with individuals involved in implementing 14 different VO-RP relationships regarding their key IdM implementation decisions and the bases for those decisions; (2) we analyzed the notes from those interviews, and determined a set of parameters and values capturing the different implementation choices in order to provide a structured VO IdM Model capable of describing a VO-RP IdM system. Further, we provide a preliminary analysis of what factors influence the IdM choices. Future work includes the extension of this analysis into guidance for new VOs and RPs in designing their IdM systems.

Our paper is laid out as follows: In Section II, we provide some background on IdM for readers not experienced in that field, and discuss how VOs have influenced IdM implementations. In Section III, we describe our interview and analysis process. Then, we present our VO IdM Model in Section IV and follow that with the VO-RP relationships that were the subjects of our interviews described using our Model in Section V. We conclude with related work, our plans for future work, a conclusion, and acknowledgments.

II. Background: Identity Management

Identity Management (IdM) involves managing identifiers and attributes for entities (who they are, how they are identified and vetted, how they are authenticated, what roles, responsibilities and access rights they have, etc.), and the trustworthy communication of that information. IdM implementations include both processes and technologies, and have a number of goals, including allowing entities to be authenticated, authorized and identified for a variety of processes (auditing, user support, accounting, etc.). Entities that are the subjects of IdM can be people, systems or processes, but in the context of this paper, we are discussing IdM for people, specifically members of the VO.

Since two of its foci are authentication and authorization, IdM is a process that is fundamental for establishing trust and managing risk. Thus, significant changes to IdM systems pose significant challenges, as organizations are sensitive to how those changes impact trust and risk.

Prior to the emergence of VOs, each RP was generally completely in control of the IdM implementation for its users - they vetted their users, credentialed them, managed their privileges, authorized their actions, and directly collected any

Funded by the US Department of Energy Next-Generation Networks for Science (NGNS) program (Grant No. DE-FG02-12ER26111). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of the sponsors or any organization.

needed additional information (attributes) about their users. As collaborations grew and needed resources from multiple providers, VOs emerged to provide a common interface to multiple RPs for users and to facilitate coordinated use of those RPs. For many VOs, this coordination included a single IdM system (or at least coordination among multiple IdM systems) to allow the users to use a single login to gain access to resources at multiple RPs as well as allow coordinated accounting, user support, and other functions.

The emergence of VOs has raised the challenging question of how the IdM process should be extended from the RP to the VO? Or, more accurately, *what parts of the IdM process should be delegated from the RP to the VO*?

The answer to this question is not all or nothing, but includes a set of possible answers depending on myriad factors. Over nearly the last two decades during which the VO has played a prominent role in scientific computing, there have been a wide variety of ways that IdM responsibilities have been distributed between the RP and VO (as the results of our interviews in Section V show).

III. Our Process: Interviews and Analysis

Toward our goal to create a VO IdM Model that captures the range of IdM implementation choices, we interviewed a number of implementers of VO IdM systems. We conducted fourteen interviews to obtain both subjective and objective information regarding identity management implementations across a broad range of VOs and RPs on which to form our VO IdM Model. We developed a semi-structured interview process [1], with questions around the following topics:

- *governance and stakeholders*: what parties had influence over the IdM choices;
- *assets and threats*: what were the biggest concerns of the parties involved;
- *user management*: what were the processes for vetting, enrolling, authenticating and authorizing users;
- *incident handling*: how were exceptional cases handed when users needed to be contacted;
- *lessons learned*: what worked well and what would be changed if it could be re-implemented.

Additionally, we supplemented the interview results with published papers, presentations or articles about the VO and RP.

We interviewed people involved with the implementations of the following VO-RP relationships (please see the Acknowledgments section for specific individuals interviewed): Engage - various, CMS - U. of Nebraska, CMS ops - various, Atlas - AGLT2, Atlas ops - various, ESGF - various, Darkside - various, Fermi Space Telescope - SLAC, LSST - various, BaBar - SLAC, LCLS - SLAC, CMS - Fermigrid, Belle II - various, and various - GRIF.

Following the interviews, we undertook an iterative process to derive a model that best fit the data. Our goal was to develop a model that allows for both the easy and clear expression of data from all 14 interviews, and provides guidance in designing a VO IdM implementation. We initially selected, based on our experience, a set of parameters and possible values. We then attempted to match our interview data to those parameters, and then iteratively refined the parameters and values to improve the quality of the matches. The quality of the match was determined subjectively by the authors based on our combined 60+ years of experience in distributed computational science, cybersecurity and identity management, and four iterations were required.

IV. Our Virtual Organization Identity Management Model

The emergence of VOs has raised the challenging question of how much of the IdM process should be delegated from the RP to the VO. The answer to this question is not all or nothing: An RP's level of trust in a VO's IdM has a range from almost none (e.g., where a VO simply directs users to some identity vetting process operated by an RP), to one where an RP has no ability to identify the individual users of a VO (e.g., the VO enrolls members and handles all direct interactions with those users). Over nearly the last two decades during which the VO has played a prominent role in scientific computing many variations of VO IdM have been implemented. The main contributions of our VO IdM Model is to enumerate the parameters and related values that comprise these variations, and organize them into a coarse but useful set of categories. We also provide some preliminary insights into what factors influence parameter values and make a particular set of values best suited to a particular VO-RP relationship.

A. The VO User Lifecycle

Finding a set of parameters to capture the options related to VO IdM was a significant challenge in developing our model. A key moment was recognizing there exist a number of discrete steps in the lifecycle from a user's enrollment into a VO, through their use of RP resources and eventual departure from the VO. We refer to these steps as composing a VO user lifecycle, somewhat akin to the "identity lifecycle," a common buzzword in the IdM field often used to describe the phasing of management tasks from user enrollment, through access and use of resources, to deprovisioning. Through our interviews, this lifecycle emerged as the core organizational layer for key IdM choices as each stage poses important decisions for flow of data and distribution of responsibilities between the parties. Namely, each stage represents a possible point where the RP can become involved with the VO's individual users instead of treating the VO as a single entity.

The stages of the VO user lifecycle we observe are:

- *Enrollment*: An initial, typically one-time process by which the user is admitted into the VO.
- *Provisioning*: Following an enrollment, the one-time creation of any state associated with the user across the VO or RPs.
- *Request*: The process by which the VO makes a request for resources from an RP to provide service to its users.

A request can be in direct response to a user's action or can be an *a priori* reservation (e.g., a pilot job).

- *Usage*: Consumption of a RP's resource by a VO to provide service to a user. This can directly follow a request or may come some time later.
- *Incident management*: Some sort of event that typically requires manual interaction with the user to resolve. This includes computer security incident response, a misbehaving user process, or a user support process.
- *Deprovisioning*: Removal of users from the VO, cessation of their right to consume resources on behalf of the VO, and possibly removal of any state or data owned by the user. (In practice, not many IdM systems implement deprovisioning and hence we do not have much data with regard to it, so it receives less attention than other stages in our Model.)

B. Our VO IdM Model: Options by Lifecycle Stage

Using the VO user lifecycle stages described in the previous subsection, we found a good fit for describing the different choices for IdM implementation that emerged from our interviews. As we describe subsequently, earlier RP-user involvement is an indicator of decreased IdM delegation by the RP to the VO. Hence, a high-level, key parameter of our VO IdM Model is at which of the lifecycle stages, if ever, the RP becomes aware of the identity of the user. Or in other words, *when does the VO pass user's identity to the RP?* Any of the lifecycle stages (except deprovisioning) are possibilities based on our observations, or the RP may never learn the user's identity. Quantification of this value provides a useful first-order description of the VO-RP's IdM relationship by expressing the degree of delegation of IdM from the RP to the VO.

Within this high-level parameter there exist finer-grained options regarding how the user identity information is managed between the VO and RP. Table I shows the finer-grained parameters we observed in our interviews, organized by VO user lifecycle.

TABLE I. USER IDENTITY MANAGEMENT OPTIONS.

VO User Lifecycle Stage	Options w/ Abbreviated Names	Notes
Enrollment	VO makes decision to enroll unilaterally (VO) VO makes decision based on negotiations with RP (VO/RP) RP makes decision (Classic)	For VO/RP we often observed RPs specify user identity credential strength. RP represents the “Classic Model” with no delegation by RP to VO.
Provisioning	VO only (entered into VOMS). Variants include shared Group account or dynamically assigned Pool account. RP state created. Variants include a User Account created (User) or just entry of user into an access control list (ACL).	The provision might be “lazy”, i.e. performed at first request. There might be considerations for “special users” in the VO
Request	RP authorizes based on per-user information (USER) RP authorizes based on VO membership or role (VO)	
Usage	Known user. Variants include use of an Isolated account (dynamic or persistent) or a shared Group account. VO member. Variants include use of an Isolated account (dynamic or persistent) or a shared Group account.	
Incident Handling	RP handles incidents (RP) RP obtains needed info from VO to handle incidents, usually user identity and contact information (from VO) VO handles incidents (VO)	Incident handling can include contacting user to resolve, or denying user access (“blacklisting”).

C. Relationship of Our Model to Trust and Risk

A goal in developing our VO IdM Model, was to understand how the IdM decisions interact with trust and risk, since these are often of concern to those making decisions regarding VO IdM implementations. Trust is a complex concept, and is subject to myriad definitions informed by work in fields including philosophy, sociology, law, psychology, and information theory. Even within the field of information security it has a variety of definitions (see, e.g., [2], [3], [4]).

In studying this prior work, we based our definition for both terms on the recent risk theory work of Philip J. Nickel and Krist Vaesen on the relationship between trust and risk [5]: *Trust is a disposition to willingly accept the risk of reliance on a person, entity, or system to act in ways that benefit, protect, or respect one's interests in a given domain.* This definition captures the relationship we see between VO and RP with regard to IdM: the more the RP chooses to delegate to the VO in terms of IdM, the more trust it has in the VO and the more risk it accepts in terms of that relationship. (We note RP may lower its overall, aggregate risk if the VO is better positioned than RP to undertake certain IdM actions and responsibilities.) RPs have in place a number of means of reducing trust and risks on the actions users are allowed to perform. At the coarse level, it is the amount of delegation of the IdM process to the VO. At the finer level, these controls are policies and attributes agreed upon with the VO, and these make up the options to the parameters described in Table I.

D. Motivating Factors for Identity Management Decisions

We turn now to a discussion about why a VO and RP might have chosen a particular set of parameters. We acknowledge our analysis of these factors is preliminary and plan to expand on this in future work.

The observed VO IdM implementations often vary from one resource to another within the same VO-RP relationship. One reason for this is that different resources have different levels of sensitivity; for example, granting access to a readonly data store might be considered lower risk than granting shell access to a computing resource. Other reasons involve technological limitations. As previously described in Section II, IdM is both process and technology, and in some cases services have varied in their adoption of new IdM technologies and hence are limited in their IdM flexibility. Grid computing was advanced in its adoption of flexible IdM technologies; however, progress in adopting advanced IdM technologies has been slower for other services such as code development, software repository access, debugging, documentation and collaboration tools (e.g., wikis). Hence, we often saw such services use a different IdM model out of technological necessity.

Outside of the constraints of technology, we noted a recurring set of factors from our interviews, external to the IdM implementation, that strongly influenced the implementation. While the number of influences is potentially vast, a few factors emerged as particularly strong or consistently represented in our interviews. As described in Section VII, our planned future work includes further analysis of these factors and development of guidance to VOs and RPs to better make IdM decisions taking key factors into account.

Observed factors influencing IdM decisions:

- *Incentive*: The relative balance of incentives between the VO and RP to make the relationship work appears to change the pattern of IdM decisions. When incentives were balanced, implementations seem to lean towards increased efficiency for both parties. When the RP was less incentivized (e.g., it was contributing cycles to a VO not critical to its mission), then either ease of operations or risk reduction for the RP would dominate.
- *Cultural and Historical Inertia:* Older relationships seem to be more dominated by the classic model where the RP controlled all IdM. These early IdM implementations tended to be more heavily controlled by the RP.
- *Scaling Needs*: Some VOs were set up explicitly to accommodate large numbers of users. In these cases, we believe there was increased delegation of IdM from the RP to the VO for the sake of efficient enrollment of VO users.

E. Relationship of Our Model to Vetting and Credentialing

Those familiar with identity management will note that our VO user lifecycle and VO IdM Model do not directly address the vetting and credentialing of users (i.e., the process of giving them a password, certificate or other electronic token for authentication). During our analysis we made a number of attempts to integrate vetting and credentialing; however, we ultimately decided that these processes are outside the VO-RP relationship, with the following caveats:

1. Credentialing and vetting often involve the VO because the VO is well positioned to vet its own users, but this is an optimization and not a requirement. We note that a user can easily come to the VO with a credential already in hand.
2. The RP may have requirements on strength of vetting and credentialing (e.g., it requires a credential from an IGTF-accredited CA [6]), in which case it is efficient for the VO to enforce that requirement on the RP's behalf at Enrollment rather than letting the user get further into the lifecycle before encountering rejection from the RP.

V. Expression of Actual VO-RP IdM Relationships

Table II shows the VO-RP relationships that were the subjects of our interviews and their expression using our VO IdM Model. The values in the table are the abbreviations from Table I.

TABLE II. INTERVIEW RESULTS CAST INTO OUR VIRTUAL ORGANIZATION IDENTITY MANAGEMENT MODEL

Context			**VO IdM Model Parameters**					
Relationship	***Resource***	***Type of Access***	***When is IdM information provided to RP?***	***Enrollment***	***Provisioning***	***Request***	***Usage***	***Incident Handling***
ATLAS & Brookhaven	Batch	Arbitrary exec	IR	VO	Group	VO	VO Group	RP
ATLAS & Brookhaven	Wiki	Web	Provisioning	VO	User	User	Known Isolated	RP
ATLAS & Brookhaven	CVS	Shell	Provisioning	VO	User	User	Known Isolated	RP
ATLAS & AGLT2	Batch	Arbitrary exec	IR	VO	Group	VO	VO Group	From VO
various & Brookhaven	Batch	Arbitrary exec	Never	VO	Group	VO	VO Group	Blacklist VO
Alice & Brookhaven	Batch	Arbitrary exec	IR	VO	Group	VO	VO Group	VO
CMS & Fermilab	Batch	Arbitrary exec	Request	VO	Pool	VO	VO Isolated	RP
CMS & Fermilab	News	Web	Request	VO	User	User	Known Isolated	RP

Context			**VO IdM Model Parameters**					
Relationship	***Resource***	***Type of Access***	***When is IdM information provided to RP?***	***Enrollment***	***Provisioning***	***Request***	***Usage***	***Incident Handling***
CMS & U. Nebraska	Batch	Arbitrary exec	Request	VO	Pool	VO	VO Slot	VO
LIGO & various	Batch	Arbitrary exec	Provisioning	VO	User	User	Known Isolated	VO
BaBar & SLAC	Batch	Arbitrary exec	Provisioning	Classic	User	User	Known Isolated	RP
BaBar & SLAC	Hypernews	Web	Enrollment	Classic	User	User	Known Isolated	RP
BaBar & SLAC	CVS	Shell	Provisioning	Classic	ACL	User	Known Isolated	RP
Belle II & KEKB	Batch	Arbitrary exec	IR	Classic	Group	VO	VO Isolated	TBD
Belle II & KEKB	Wiki	Web	Enrollment	Classic	User	User	Known Isolated	TBD
Belle II & KEKB	CVS	Shell	Provisioning	Classic	User	User	Known Isolated	TBD
Belle II & PNNL	Batch	Arbitrary exec	IR	VO	Group	VO	VO Isolated	TBD
FST & SLAC	Data	Web	Provisioning	Classic	User	User	Known Isolated	RP
FST & SLAC	Wiki	Web	Enrollment	Classic	User	User	Known Isolated	RP
LSST & NCSA	Batch	Arbitrary exec	Provisioning	Classic	Group	VO	VO Isolated	TBD
LSST & SLAC	Wiki	Web	Enrollment	Classic	User	User	VO Isolated	RP
ENGAGE & various	Batch	Arbitrary exec	Request	VO	Group	VO	VO Group	VO
various & CRNS/LAL	Batch	Arbitrary exec	Request	VO	Group	VO	VO Group	from VO
Darkside & various	Batch	Arbitrary exec	TBD	TBD	TBD	TBD	TBD	TBD
various & Fermilab	Batch	Arbitrary exec	Provisioning	VO	Group	VO	VO Isolated	RP
ESGF & various	Data	Web	Request	VO	ACL	VO	VO Group	----
ESGF & various	Restricted data	Web	Provisioning	VO	ACL	User	VO Isolated	----
LCLS & SLAC	Batch	Arbitrary exec	Enrollment	VO	User	User	VO Isolated	RP
LCLS & SLAC	Data	Shell	Enrollment	VO	User	User	VO Isolated	RP
various & U Nebraska	Batch	Arbitrary exec	Never	VO	Group	VO	VO Group	VO
FUSION & various	Batch	Arbitrary exec	Provisioning	VO	User	User	Known Isolated	RP
Various science gateways & XSEDE	Batch	Restricted exec	Never	VO	Group	VO	VO Group	VO

VI. Related Work

Landau and Moore's work, "Economic Tussles in Federated Identity Management" [7], discusses the relationship between perceived risks and challenges for relationship formation in the context of IdM. With more to lose, stakeholders become particularly attuned to what they gain and how responsibility is distributed. This informed our understanding of factors that influence how IdM decisions are made in the VO context.

The Federated Identity Management for Research Collaborations paper [8] provides a number of studies of VOs and their needs for federated identity. This work helped us shape our interview process.

SCI: A Trust Framework for Security Collaboration among Infrastructures [9] is an ongoing effort to define a broader set of standard policies for VO-RP interaction. This work is targeting a specific set of requirements, and hence will represent on particular set of choices in our VO IdM

Model (plus choices outside the context of our Model since the work is broader tham IdM).

The Open Science Grid made a presentation to the MAGIC committee [10] on how its resource providers consume identity information. Since the RPs in this presentation were anonymized, it wasn't directly usable by us, but this work did help shape our interview process.

Haidar has published a study of VO architectures [11], which analyzes three theoretical IdM systems and a paper on modeling of VO IdM that introduces the Audited Credential Delegation (ACD) mechanism [12]. These works represent more of a requirements analysis for the ACD implementation and less of a generic model such as this paper presents.

Lin, Vullings, and Dalziel proposed a "Trust-based Access Control Model for Virtual Organizations" [13]. This work is similar to our model, with an attempt to quantify trust decisions based on the type of resource access. However, it focuses solely on access control decisions rather than the entire VO-RP relationship.

VII. Future Work

Our VO IdM model was based on the results of our 14 interviews. Future work includes further validating our model by reorganizing our interview process around the model and undertaking more interviews in the context of the model. We also will continue our analysis of motivation factors to strengthen our guidance to VOs and RPs in terms of how their relationships are best cast to meet their requirements in an implementation based on the VO IdM model. We also hope to test that guidance by working closely with emerging VOs establishing their IdM systems. We plan to explore adjusting the model to accommodate new types of RPs being utilized by VOs outside of academia and government laboratories (e.g., commercial clouds).

VIII. Conclusion

Our goals are to provide both a common language for VOs and resource providers (RPs) to describe IdM implementations in the context of VOs, and provide guidance to those parties in making implementation choices to best meet their trust and risk requirements. Without related tools, VO IdM implementations are hampered due to complexity, a lack of overarching decision frameworks, and reduced clarity regarding the repercussions of decisions.

This paper takes steps toward achieving those goals. We have presented the results of a set of 14 interviews we conducted with individuals from virtual organizations (VOs) and resource providers (RPs) exploring how they implemented identity management (IdM). We analyzed the results of those interviews to construct and present in this paper our model describing a VO IdM system, which captures how VOs and RPs relate in terms of IdM. We also included a preliminary analysis of the motivations that have led to different implementations within the model, providing some preliminary guidance to future VOs and their RPs. Our future work includes further validating and refining the Model and developing guidance by working with VOs.

Acknowledgments

We thank the US Department of Energy Next-Generation Networks for Science (NGNS) program (Grant No. DE-FG02-12ER26111) for funding this effort. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the sponsors or any organization.

We thank the following interviewees for their time and insights: Brian Bockelman, Univ. of Nebraska; Concetta Cartaro, BaBar; Keith Chadwick, Fermigrid; Richard Dubois, FST and LSST; John Hover, ATLAS Ops; Tony Johnson, FST and LSST; Michel Jouvin, GRIF; Thomas Kuhr, Belle II; Steffen Luitz, Darkside; Shawn McKee, AGLT2; Amedeo Perazzo, LCLS; Igor Sfiliogi, CMS Ops; Alex Sim, ESGF; Mats Synge, Engage.

We also thank Jim Basney and Drew Simshaw for discussion and insights which improved this work.

References

[1] C. Robson, *Real World Research: A Resource for Users of Social Research Methods in Applied Settings, 3rd ed.* Chichester, West Sussex, United Kingdom: Wiley, 2011, p. 280.

[2] A. Jøsang and S. Lo Presti, "Analysing the relationship between risk and trust," presented at the *Second International Conference on Trust Management (iTrust 2004)*, Oxford, UK, 2004.

[3] L.S. Gallege, D.U. Gamege, J.H. Hill, and R.R. Raje, "A study of trust in distributed software systems," *ACM Computing Surveys*, vol. 9, no. 4, article 39, March 2012.

[4] M. Blaze, J. Feigenbaum, J. Ioannidis, and A.D. Keromytis, "The role of trust management in distributed systems security," in *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, J. Vitek and C.D. Jensen, Eds. Berlin: Springer-Verlag, 1999, pp. 185-210.

[5] P.J. Nickel and K. Vaesen, "Risk and trust," in *Handbook of Risk Theory*, S. Roeser, R. Hillerbrand, P. Sandin, M. Peterson, Eds. New York: Springer, 2012, pp. 858-873.

[6] The International Grid Trust Federation. http://www.igtf.net/

[7] S. Landau and T. Moore, "Economic tussles in federated identity management," *First Monday*, vol. 17, no. 10, Oct. 2012. Available: http://journals.uic.edu/ojs/index.php/fm/article/view/4254/3340

[8] D. Broeder, et al., "Federated identity management for research collaborations," CERN-OPEN-2012-006, Apr 23, 2012. Available: http://cds.cern.ch/record/1442597?ln=en

[9] K. Chadwick, et al., "SCI: A trust framework for security collaboration among infrastructures," Feb. 8, 2013, draft ver. 0.95. Available: http://www.eugridpma.org/sci/

[10] M. Altunay, "How OSG Resource Providers Consume Identity Information", unpublished presentation to the MAGIC committee, Dec. 4, 2012.

[11] A. N. Haidar, et al., Formal modelling of a usable identity management solution for virtual organisations, in *Proc. Second Workshop Formal Aspects of Virtual Organisations* 2009 *(FAVO2009) EPTCS 16, 2010*, J. Bryans and J. Fitzgerald, Eds. pp. 41-50.

[12] A.N. Haidar and A.E. Abdallah, "Comparison and evaluation of identity management in three architectures for virtual organizations," in *IEEE Proc. Fourth Int. Conf. Information Assurance and Security*, pp. 21-26.

[13] A. Lin, E. Vullings, and J. Dalziel, "A trust-based access control model for virtual organizations," in *IEEE Proc. Fifth Int. Conf. Grid and Cooperative Computing Workshops (GCCW'06).*