

# Federated Global Identity Management: Research Agenda & Outcomes

Jawed Siddiqi, Babak Akhgar and Mehrdad Naderi: Sheffield Hallam University (UK)  
Wolfgang Orth: Fraunhofer Institute for Secure Information Technology (Germany)  
Norbert Meyer: Poznan Supercomputing & Networking Center (Poland)  
Miika Tuisku: University of Helsinki (Finland)  
Gregor Pipan: XLAB (Slovenia)

Name of Conference: **The 2006 International Conference on Grid Computing & Applications (GCA'06)**

*Abstract - The paper define the problem situation of digital identification in ICT infrastructures from three perspectives: systems, end user and technology. It details the research agenda and outcomes in terms of: a collaborative research cycle, the project goals, high level requirements and features of the proposed system. Finally, the FeGIMa vision is elaborated in terms of two impacts, that outlines the benefits that accrue to heterogeneous global computing infrastructures: the first, being scientific and technological, the second being socio-economic together they outlines the impact on the vision Global Computing (GC). For the disparate community of global computing stakeholders the freedom obtained through the proposed technically innovative FeGIMa project results in the simplicity of "Single Sign on and Single Service Authentication - SSO& SSA" thereby directly contributing to realising the vision of Information Society for All.*

Keywords: **FEDERATED GLOBAL IDENTITY**

## 1. Introduction

Society appears to be moving towards a vision as captured by the ubiquitous phrase "Information Society for All". In particular, the EU vision, envisages the citizen having more and more services being delivered online: eCommerce, eGovernment, eHealth etc. A necessary requirement, so that they are readily available to all, is that these services are secure and trustworthy.

It has been noted that the EU approach to electronic security can be seen from three inter-related, termed here as the "3P", perspectives:

- protection of citizen data and their privacy
- prevention from intrusion into information networks
- prohibition of hackers committing cyber-crime

In order to explore the what and how of secure and trustworthy services we begin by considering two fundamental notions that we regard to be at the heart of all these activities, they are: digital identity and digital identification. We follow and build on the work in the EU IST funded project FIDIS, Future of Identity in the Information Society, project. In its deliverable D2.1 "Inventory of topics and clusters" they rightly point out that identity and identification are two distinct but related concepts. Indeed, identity is the information

that characterises an individual via set of attributes in different situations, whereas, identification relates to a set of mechanisms for detecting information relating to identity during traversal and interaction in global (i.e. a multiplicity of distributed heterogeneous) ICT infrastructures; such as Grid, Web and Wireless & Mobile. The focus of this paper is on complexities of identification rather than the vagaries of identity which are being addressed in FIDIS.

Presently, identification within one infrastructure i.e. Grid continues to be significant challenge. Indeed, to ensure secure and trustworthy communications a successful interaction between the service requestor and service provider has to take place, for this to happen the security and trust model must provide mechanisms by which the authentication credentials (ie identity information) from the service requestor can be translated/authenticated by the service provider so that trust and security relations have been established.

Therefore, digital identification considerations in multiple distributed heterogeneous ICT infrastructures, hereafter termed global ICT infrastructures, clearly necessitates fundamental research that is highly relevant to current needs of society. For this reason alone our current Federated Global Identification Management (FeGIMa) Framework research project is vital because it is aiming to develop a framework for digital identification within a global ICT infrastructure.

The Primary aim of FeGIMa is to advance Federated Identification towards a global infrastructure to counter what has been termed in the EU IST Framework VI programme as “dystopic aspect of a disarray of unrelated and incompatible Global Computers”. Towards this end, taking-off from the Grid as one important set of - partly incompatible - instances of the Global ICT infrastructures. FeGIMa focuses on, initially known, but is open to new infrastructures of Global Computing paradigm. Examples of known infrastructures, addressed in FeGIMa from a GC focus are the Grid, the Web etc. New GCs in the given context are for example “converged mobile communication infrastructures”. FeGIMa, therefore can be seen to counter “dystopia” by a Federated Global Identification Management Framework through enhanced Interoperability.

We are conducting research into the formulation of the architectural blueprint necessary to provide a Global identification service across global ICT infrastructures integrating that of the Web and the Grid and introducing the concept of what the EU IST Framework V initiative refers to as ‘protected GC infrastructure’. Such a platform implies a secure vertical integration between heterogeneous grid platforms but more significantly creates the condition for horizontal integration i.e. interoperability of various global infrastructures (the Internet, the Web and the Grid) with common services i.e. the creation of new secure and trustworthy global and interoperable services.

The research proposed is both fundamental and highly innovative because the FeGIMa framework manages individual and organisational identification with their disparate security mechanisms. It does so for the variety and diversity of global ICT stakeholders through the formulation of a sufficiently abstract/high-level architectural blueprint that frees them from having to be constrained to the same (i.e. one type fits all) technologies for authentication. For the disparate community of global computing stakeholders the freedom obtained through the proposed technically innovative FeGIMa framework results in the simplicity of “Single Sign on and Single Service Authentication - SSO& SSA” thereby directly contributing to realising the vision of Information Society for All.

The FeGIMa vision is elaborated in terms of three impacts: the first, being strategic that outlines the impact on the world; the second, being scientific that outlines the impact on Global Computing (GC) vision, and finally technological, that outlines the impact on the benefits that accrue to heterogeneous global computing infrastructures.

The FeGIMa project aims to deliver a reference framework and the underlying reference architecture that underpins the framework along with a service based identity management “showcase” that would exhibit higher levels of interoperability between the global computing infrastructures of the Internet, the Web, and the Grid as well as the heterogeneous grid

middleware implementations. In doing so, it will showcase the broadening required for the adjective ‘global’, in that we move between existing vertical integration models and amongst the global computing infrastructures noted above to share resources without the necessity to adopt the same technologies for identity management (e.g. directory services) and identification (authentication and authorisation).

The research was led through a collaborative effort by the following four partners: Sheffield Hallam University (UK), Fraunhofer Institute for Secure Information Technology (Germany), University of Helsinki (Finland) and Poznan Supercomputing & Networking Center (Poland) leading to the proposed development of the proposed Trust-Me framework. This was then distributed for peer review and comments to our industrial partners that included Sun Microsystems (Belgium), Telecom Italia (Italy), Telefónica Investigación y Desarrollo (Spain) Valimo Wireless (Finland) and an SME XLAB (Slovenia). Therefore, the proposal benefits from being a true European wide collaborative effort in development and equally importantly a peer to peer critique between leading academic institutions and key industrial partners involved in security and telecommunications. In the paper here we provide an overview of a research agenda that is working towards a framework for Federated Global Identity Management (FEGIMA). In a companion paper we detail the progress so far on the technical aspects of the Framework for Federated Global Identity Management.

In the next section, we define the problem situation in terms of digital identification in ICT infrastructures, briefly outlining three perspectives: systems, end user and technology. The remainder of the paper details the research agenda. First, a collaborative research cycle that is being employed. Second, the project goals as well as the high level requirements and features of the system to be developed. Finally, the FeGIMa vision is elaborated in terms of two impacts, that outlines the benefits that accrue to heterogeneous global computing infrastructures: the first, being scientific and technological, the second being socio-economic together they outline the impact on the vision Global Computing (GC)

## 2. Digital Identification in ICT Infrastructures

To meet the challenge of current industry trends such as growth in business-to-business (B2B) commerce, business to customer (B2C) and even customer to customer (C2C) increased need for mobility and for persistent connectivity, organisations are extending internal systems to external users which in turn will lead to future oriented value chains. To this end, organisations are creating inward and outward focused

information systems (IS) that integrate contributing business constituents into their core business processes.

From a systems perspective; as the above boundary between internal and external focused information systems continues to blur, the traditional security perimeter is fast becoming eroded. That is, whilst organisations require to protect this security boundary, they need to open their data and business critical systems to tap into the value gained from their extended value chain noted above, thus making these accessible, independent from geographical location and therefore susceptible to security infringements. Organisations are thus challenged with two seemingly opposing trends, the need to increase access to information and the need to maintain security in a manner that will generate and support new business opportunities nationally and internationally.

From an end user perspective; all users create digital identities (DID) as they traverse cyberspace. Stakeholders employ different user names, passwords and other identifying attributes in various online contexts due to practical limitations or out of a desire for anonymity. This authentication data (passwords or pins) have to be memorised, since a unique and ubiquitous universal DID concept is far from being realised in the cyberspace. At the same time, every organisation creates identities to provide individuals with secure access to online resources and services. As gaining access to distributed resources, including applications, becomes increasingly vital, the ability to manage identity effectively becomes a paramount concern. Web services, and the grid which have a potential to enable even greater business integration and value further magnifies this problem of effective identity management.

To meet the new challenges noted above, emerging federated identity and the standards for federation are recognised as a key ingredient in the re-configuration of systems to accommodate the secure adoption of more distributed and transparent computing models. These current standards, established by OASIS (SAML) [1], Liberty Alliance Project (ID-FF, ID-WSF and ID-SIS)[2], Microsoft and IBM [3], (WS-Roadmap) and Internet2 (Shibboleth)[4] define mechanisms for sharing identity information between domains. Our work builds on and extend the current state of the art research that will enable organisations to not only be able to work securely with autonomous internal and external strategic business units, for example, within a trusted domain inside an the enterprise, but also with third party identity services - amongst other trusted domains.

From a technological innovation perspective, the emerging identity federation standards rely heavily on web services architecture. Because both web services framework and identity are evolving along similar architectural paths. The former offers the foundation that enables the realisation of virtual organisation paradigm, whilst identity management secures it. Moreover, the convergence towards a common

encoding format for all types of data (XML) and the underlying protocol for transporting the latter (SOAP) taken along with Web services framework is resulting in the creation of a standard software communication bus. The emergence of this bus has profound implications for identity exchange. Instead of having to agree on one identity and security system that suits all (the notion of one type fits all). We will have enhanced the state of the art by enabling differing security frameworks to exchange authentication and authorisation assertions provided these security frameworks can consume and produce the standard assertion format (e.g. SAML), they can inter-operate in a federated model automatically.

### **3. The Research Agenda: Proposal**

#### **3.1 Collaborative Research Cycle**

The project has been initiated by a joint Industry & Academia research initiative under the EU IST effort. It was agreed that due to the nature of the project the best mode of inquiry is action driven collaborative research as stated by Akhgar [5&6]. The iterations cycles during the project discussion process in terms of confirmation, clarification, adjustment, amendment and changes of the key requirements elicited were used as evidence of practical effectiveness of an underlying theory for construction of our architecture without specific organisational narratives. The latter enabled us to address the risk and shortcoming of action research in terms of being too focus on specific organisation and limitation of findings in terms of scope as stated by Peters and Robinson [7] and Seashore and Taber [8]. Furthermore, the adapted iteration principal in the construction of our architecture reduced the risk of our subjectivism and over positivistic interpretation of the requirements by embodying a multiplicity of views, commentaries and critiques, leading to finalise requirements for construction of our FeGIMA framework.

The project team lead by academic partners established the theoretical framework guiding the “action research” in their capacity as the leaders of the action team through collaborative workshops with the members of action team (representatives from industry and academia). During initial workshops the key security requirements obtained were discussed, clarified and challenged (see 3.1). At the start of the project the workshops focus changed to defining the deliverables, milestones and their iterations and increments. Further three workshops were arranged and ran to learn about standards, best practices, goals and objective, and other projects. The workshops served as an effective instrument to capture the collective mental construct of the action team for construction of the architecture. The collective mental construct of action team in

relation to the project reflected in the contextualisation of FeGIMa project.

From action research perspective the aim of workshops was to create and establish “reflection-based learning” of the action team. Based on the research by Mezirow [9] we have established set of three areas of reflecting learning. The contextualised view of reflecting learning in the project is as follows:

1. **Content reflection:** Discussing, evaluating and understanding of the research diagnosis including the problem situation (within federation), problem frames validity of project industrial context, the key requirements and the underlying assumptions about the nature of Federated Global Identity Management
2. **Process reflection:** Understanding and validating the action planning (including effectiveness of action team and further requirements for successful construction of the architecture), project conduct, evaluation principals, and strategies for future research and collaboration with other projects
3. **Premise reflection:** learning about to what extend Industry specific behaviour (in terms of politics, standards and norms) influenced construction of our architecture. Although we have to acknowledge from “premise reflection” perspective learning was limited due to a number of factors namely team structure, research focus, and time restriction.

The “boundary of concern” for the research reported here was agreed as secure ICT for mobile and wireless devices domain. In order to assess the impact of the FeGIMa architecture two high level assessment relating to the Scientific and Technical contribution that results from the delivery of the FeGIMa outcomes as well as the potential socio-economic impact that will result from the deliverables of the project.

### **3.2 Goals, Requirements and Features**

The specific aim of the proposal addressed in this paper is the development of a framework for digital identification in a global ICT infrastructure. By analysing the complete spectrum of technical and business issues surrounding Federated Global Identity Management, the FeGIMa project will address the following goals: expanding the circle of trust and privacy, interoperability standards, and virtualisation of resources, these goals are elaborated as follows:

#### ***G1: Expanding Circle of Trust and Privacy***

As identity authentications and attributes are shared within the identity federation, organisations are compelled through privacy legislation to respect each individual’s privacy rights and preferences. Within identity federation an individual is subjected to differing privacy policies and must be aware of such fact as he moves from one trusted domain to the next within a single sign on (SSO) interaction. Therefore, addressing the issue of quality identity interaction and accountability as well as measures for handling and resolving disputes and intrusions within the larger context of federation is necessary challenge that needs addressing.

#### ***G2: Building On Interoperability Standards***

Technical interoperability is the cornerstone of efficient wide-scale federation, without which the full potential of identity federation will never be achieved. Addressing interoperability requires cross GC infrastructure cooperation to ensure that the resulting solutions address the wide range systems with which it must integrate.

#### ***G3: Virtualisation of Resources***

Virtualisation of resources for computationally complete transactions built on FeGIMa goal G2 as an overlay computer. Where, virtualised resources offered by resource providers can be mapped to the rights of an individual for use on a permanent or temporary basis. Moreover, the resource usage and management will be greatly simplified through FeGIMa’s provision of a transparent layer, which unifies heterogeneous virtualised resources.

#### ***Requirements and Features***

As a first step in the development of the FeGIMa framework we make explicit the relationship between identity and identification by introducing three notions: identity owner (user identity), identity provider (where the identity is hosted) and the identity consumer (where identification takes place) see Figure 1. Contracts exists between the identity owner (i.e. the user) and the identity provider where the contract dictates conduct and net-etiquette from the user and privacy and trust from the identity provider. The same exists between the identity provider and identity consumer.

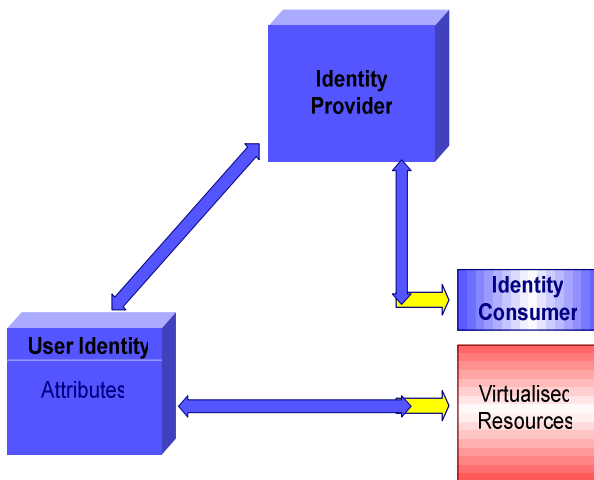


Figure 1: FeGIMA User, Provider, Consumer relationship

In order to reach the above goals, the FeGIMA project will ensure that the following requirements/constraints explicated from the goals relating to identity from the user, provider and consumer perspectives are satisfied.

### ***Standards, Scope & Constraints***

- Ensure a common vocabulary regarding accountability for the representation, negotiation and actions of identity: owner, provider and consumer.
- Ensure that an extensible attribute vocabulary is provided.
- Ensure a common protocol for asserting and authenticating.
- Ensure a common a negotiation protocol to allow owners to control the privacy and security terms under which they are willing to assert identity or exchange information.
- Ensure open standards for interoperability and extensibility for universal data representation and schema definitions for service and protocol definitions
- Ensure that standards adopted/developed support multiple trust levels so that simple transactions can be kept simple and identity owners need only be certified to the trust level necessary for the transactions in which they engage.

### ***Features, Functions & Properties***

- Ensure support for identity owners to extend data or message definitions as required/needed for specialised uses.
- Ensure that, there is no limit to the attributes that may be associated with an identity.

- Ensure access to all registration and certification authorities.
- Ensure that a common protocol for any number of registration authorities is provided.
- Ensure that identification does not disclose details that can hamper anonymity.
- Ensure support for anonymity and pseudo-anonymity for protection of personal privacy when assertion of real-world identity is not required or desired.

In the companion paper we present the details of the FEGIMA framework, the architecture and the challenges & innovation required to achieve the project goals. However, to illustrate the impact of the outcomes of the FEGIMA proposal we consider two types in terms of both the scientific & technical as well as the socio-economic impacts

### **3.3 Impact**

At the highest level the outcome from the FeGIMA project for both sets of stakeholders: service user (identity owner) and service provider (identity consumer) is the seamless submission of jobs from which the following benefits accrue:

- Only one authentication is necessary (Single Sign On SSO)
- Service User can be assured, that only information that s/he has approved is passed to the service provider
- Service Provider can be assured, that the security and usage policies they define are enforced

#### **3.3.1 Scientific and Technical Impact**

FeGIMA's unique approach to tackle the identity and identification problem in global distributed computational systems through the identity owner (the user), the identity provider and identity consumer will devise innovative theories in security and resource management. Additionally, the project aims to deploy the framework, which will demonstrate the strength of federated identity theories. The theoretical model and linguistic issues (syntax and semantics of federated identity) will be defined to support the management of individual and organisational identities with their disparate security mechanisms.

The term federated itself holds the semantic of horizontal integration (i.e. interoperability) of various global computing infrastructures with common services. Additionally, given the need for same within the global computing infrastructure of

the grid i.e. vertical integration between heterogeneous grid middleware implementations, the major contribution of FeGIMa project is the horizontal and vertical integration of global computing infrastructures of the internet, the Web and the Grid encompassed in one framework, in order to provide a user with the virtual transparency to all the resources, available to him or her. Therefore, FeGIMa will provide uniform identity services for the global ICT infrastructures of the Internet, the Web and the Grid that will enable user mobility within the digital globe and easier co-operation between different computational infrastructures, provided through FeGIMa federated global identity framework..

As the FeGIMa project addresses the issue of secure identity management in global distributed systems, with providing federated global identity management framework, there is an immediate impact on several initiatives addressing the problem of resource brokerage (EU-DataGRID project, Grid Resources Distributed and Parallel Systems - University of Innsbruck, EZ-GRID), It will therefore extend the existing initiative with adding a layer allowing a transparent access to greater range of resources located within interconnected heterogeneous distributed systems.

### **3.3.2 Socio-economic Impact**

As stated previously the task of obtaining a new certificate and managing a set of certificates for various purposes is a major obstacle to the global ICT vision of easy accessibility to all.

The federated global identity management project proposal has the potential to solve these problems by providing open standards and protocols with the ability to span and move between different virtual organisations and infrastructures, built into it from the start. So, it will help to create a global environment of cooperating users and services, while enabling particular security domains to have their policies managed by themselves and increase the trusted relationships among the users in different virtual organizations of various middleware platforms. The deployment of a federated identity infrastructure limits an organisations vulnerability to security attacks.

Within an enterprise, economic goals necessitate increased sharing information between the business partners and its customers thereby impacting the importance of security used in communication. Federated identity could provide single pervasive security standard for B2B applications that sets mutual confidence between the business partners and so bring substantial cost savings, operational efficiencies, and increased security. In addition to this, corporate acceptance of Grid technology is

greatly enhanced as the proposed framework will help to enhance IT-Security compliance to standards and acts, such as Basel II and Sarbanes-Oxley.

Many types of information must be shared across government and organisational boundaries. The common framework to ensure that this interoperability is trusted and secure is a requirement within agencies, among organisations, and even between nations. A federated architecture now allows systems to interoperate while maintaining their autonomy. Within a government to citizen communication, various government departments and agencies give citizens and businesses access to on-line services through their e-authentication initiatives. To avoid any generalised interconnection of public files containing personal information, the federated approach is ideal: it ensures that data is not duplicated in a single central database.

To generalise across these audiences, the benefits of implementing FeGIMa are as follows: stronger security, trust and risk management; improved alliances, both within and between organisations, through interoperability; cost avoidance, cost reduction through increased operational efficiencies because of faster response time for critical communications; and significant revenue growth through development of strategic offerings.

### **Conclusion**

The results of the FeGIMa project will enable the next generation of grid middleware one should no longer rely on the basic functionality of the traditional Internet. It should foster the utilisation of the new capabilities of the next generation Internet designed with the mobile and roaming user in mind. Simply using the mobile Internet is not enough because of various limitations partially described in the previous section. One has to establish communication points between the different layers identified and enhance their functionality in order to serve the upper layers in a more efficient way.

Moreover, the FeGIMa approach for establishing a federation of identity management systems will develop the necessary communication links between the network layer and higher layer for the grid, thereby establishing the required communication links between the identity management platform to the application layer. This enables an integrated security model which stretches from the network layer up to the application layer. Once this is achieved it will then be extended so that it is integrated with the Web through providing the necessary services and high level interfaces to allow for integration with existing results for federated identity management systems in the Web.

It could be argued that the results of the proposed research contribute to strengthening the social cohesion because users will find that they will be able to seamlessly traverse all these disparate global ICT infrastructures for various application domains such as e-Government, e-Business, e-Citizen. Therefore these services will become more attractive for the user, friendlier and easier to manage. Moreover as we have argued the outcome of FeGIMa can contribute indirectly to sustainable growth and improving competitiveness both of large and small businesses All these attributes contribute to the trust in the knowledge society and the vision of “Information Society for All”.

#### 4. References

- [1] OASIS “Security Assertion Markup Language V1.1” <http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf>
- [2] Liberty Project [www.projectliberty.org](http://www.projectliberty.org)
- [3] IBMWSSecurityandRoadMap <http://www-106.ibm.com/developerworks/webservices/library/ws-secmap/>
- [4] Shibboleth <http://shibboleth.internet2.edu/shib-intro.html>
- [5] Akhgar, B (2002 ); Software Engineering processes in practice, A survey of 50 SW Eng project, RET Vol 2, No 4.
- [6] Akhgar, B (2003); Information Systems Research, An action research perspective SHUWP2. 2003
- [7] Peters, M. and V. Robinson (1984); The Origins and Status of Action Research, The Journal of Applied Behavioral Science, V.20, No.2, pp. 113-124.
- [8] Seashore and Taber (1976); Action research and generation of human knowledge, Human relations, Vol 46, No 11. [in Gustavsen B pp:1361-66]
- [9] Mezirow, J (1991); Transformative dimensions of adult learning, CA: Jossey-Bass