Towards a Framework for Federated Global Identity Management*

Mehrdad Naderi[1], Jawed Siddiqi[1], Babak Akhgar[1], Wolfgang Orth[2], Norbert Meyer[3], Miika Tuisku[4], and Gregor Pipan[5]

(Corresponding author: Jawed Siddiqi)

Informatics Group, Sheffield Hallam University, Sheffield S1 1WB, UK[1]
Fraunhofer Institute for Secure Information Technology, Germany[2]
Poznan Supercomputing & Networking Center, Poland[3]
University of Helsinki, Finland[4]
XLAB, Slovenia[5]
(Email: j.i.siddiqi@shu.ac)

(Selected paper from ITNG 2006)

Abstract

This paper reports on research being conducted 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 proposed research is both fundamental and highly innovative because the FeGIMa framework manages individual and organizational identification with their disparate security mechanisms. It does so for the variety and diversity of global ICT stake-holders 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 stake-holders 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 realizing the vision of Information Society for All.

Keywords: Federated identity management, global infrastructures, grid

*A preliminary version of this work appeared in proceedings of international conference on Information Technology: New Generations (ITNG 2006).

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, eGoverment, 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 characterizes 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 organizational identification with their disparate security mechanisms. It does so for the variety and diversity of global ICT stake-holders 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 stake-holders 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 realizing the vision of Information Society for All.

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).

In the paper here we provide a progress report on the initial research work in the form of a federated global identity management framework and an assessment of its impact.. Section two provides a selected tour of the background material from which the framework is formulated. It focuses on: research work on federated identity and specifically identification mechanisms relating authentication and authorisation for the Web and grid infrastructures. Additionally, it provides a table of related projects. Section three outlines a partial composition of the FeGIMa framework, highlights the innovation in the framework and the assess its potential impact.

2 Digital Identification in ICT Infrastructures

2.1 Problem Situation Defined

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) [7], Liberty Alliance Project (ID-FF, ID-WSF and ID-SIS) [4], Microsoft and IBM [2], (WS-Roadmap) and Internet2 (Shibboleth) [8] 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.

2.2 State-of-the-Art Research on Digital Identification

The emerging debate over identification and the selection of technology to authenticate individuals and enterprises alike is among the most important issues that is shaping the information age today. Clearly, the concept of identity is far broader than the mere content of a name. While names and naming protocols are a critical element of identity, in that they provide the means to distinguish one individual from another, the underlying relevance, role, context and meaning attributed to a given individual can only be gleaned by reference to other factors. In the human space, this is due to people existing in many social, economic, political, cultural and other dimensions concurrently. Whilst in the digital space the varying architectures (legacy and new) and underlying enabling technologies pose a similar dilemma. In defining the identity of a person be it in human or digital spaces which is termed as virtual identity is a multi-faceted complex problem.

The following surveys the relevant issues relating to identification or identity management systems both in the public and private sectors. One key similarity is that both the public and private sectors wish to enable a system that will allow an end user (whether an individual or organisation) to enjoy the convenience of "single sign-on." (SSO) whilst increasing the opportunity to discover fraud against the systems. It remains to be seen whether there are systems and processes that can be used across both sectors. While current architectures appear to be primarily or exclusively suitable in one or the other sector, it is clear that ultimately there will be a sufficient demand for cross-sector interoperability that common-denominator solutions will be required.

Presently federated identity within one global computing infrastructure e.g. Web space continues to be a significant challenge that is the focus of sizeable volume of research. However, in contrast the research into federated identity in the grid space is not so sizeable.

2.2.1 Electronic Identity Management on the Web

In this section we review key aspects of work, relevant to FeGIMa, for two of the key governing bodies that are striving towards standardisation for identity management on the Web, namely Liberty Alliance and Shibboleth.

Liberty Alliance:
The Liberty Alliance [4] is a consortium of more than 150 organisations that develops specifications for federated identity management. It is working on the development, deployment and evolution of an open, interoperable standard for network identity where privacy, security and trust are maintained.

Liberty Alliance contributions towards federated digital identity management has been the development of three specifications:

- Identity Federation Framework (ID-FF); enables identity federation and management through features such as identity/account linkage, simplified sign on and simple session management.

- Identity Web Services Framework (ID-WSF); provides the framework for building interoperable identity services, permission based attribute sharing, identity service description and discovery and the associated security profiles.

- Identity Services Interface Specifications (ID-SIS) enables interoperable identity services such as identity profile services, alert services, calendar services, wallet services, contacts services, etc.

Federated identity and attribute servers are the solution used by Internet2 [8] projects and were developed for individual virtual organizations especially within the European Data Grid (EDG) [1]. Within federated identity management authentication depends on the notion of identity. The Liberty Alliance project's Identity Federation Framework ID-FF specifies a third party authentication model, where individual services rely upon assertions (SOAP messages carried over HTTP) generated by an identity provider. Thus, the service is not required to directly authenticate the user, but rather an entity whose sole responsibility is to identify the user based on direct authentication. This model thus requires that the service provider trusts the identity provider.

The Liberty Authentication Service in the GC infrastructure of the Web as an exemplar allows SOAP client applications to authenticate to the service via any of the authentication models specified by the IETF's Simple Authentication and Security Layer specification, thus standardising the authentication methods used.

Liberty explicitly accommodates identity provider use of arbitrary authentication mechanisms and technologies. Different identity providers will choose different technologies, follow different processes, and be bound by different legal obligations with respect to how they authenticate users. The choices that an identity provider makes here will be driven in large part by the requirements of the service providers with which the identity provider has federated.

Within the context of Liberty Alliance Web Service Framework, for identity providers and service providers to communicate with each other, they must a priori have obtained metadata regarding each other. These provider metadata include items such as X.509 certificates and service endpoints.

When sharing a globally known identifier among separate organisations, the users privacy may be compromised. Liberty allows the creation of opaque privacy-protected name identifiers, which may cross organisations without compromising the privacy of the user or leaking data.

Shibboleth:
Shibboleth [8] is a joint project of Internet2/MACE (Middleware Architecture Committee for Education) and IBM. Its focus is to investigate architectures, frameworks, and practical technologies to support inter-institutional sharing and controlled access to Web available services. Shibboleth focuses on inter-institutional resource sharing within academia, but the project is relevant to many business settings as well. The project will produce an analysis of the architectural issues involved in providing such inter-institutional services, given current campus realities and the current state of relevant standards. It will also produce a pilot implementation to demonstrate these concepts.

Shibboleth utilises frameworks for multiple, scalable trust and policy sets, termed as Clubs, to specify a set of parties who have agreed to a common set of policies. This moves the trust framework beyond bi-lateral agreements, while providing flexibility when different situations require different policy sets. It does so by making use of open SAML [7] for the message and assertion formats, and protocol bindings. Key concepts within Shibboleth include:

- Federated Administration: The originating campus provides attribute assertions about the user to the target site. A trust fabric exists between these, allowing each site to identify the other, and assign a trust level. Originating sites are responsible for authenticating their users, but can use any reliable means to achieve this.

- Access Control Based On Attributes: Access control decisions are made using those assertions. The collection of assertions might include identities, however, many situations will not require this (eg accessing a resource licensed for use by all active members of the campus community or accessing a resource available to students in a particular course).

- Active Management of Privacy: The original site and the user, control what information is released to the target. A typical default is merely "member of community". Individuals can manage attribute release via a Web-based user interface and are no longer at the mercy of the target's privacy policy.

2.2.2 Electronic Identity Management in the Grid

Grid computing has emerged as an important new field, distinguished from conventional distributed computing by its focus on flexible, secure, coordinated resource sharing among dynamic collections of individuals, organisations and resources. This sharing is, necessarily highly controlled, with resource providers and users defining clearly and carefully what is shared, who is allowed to share and the conditions under which this sharing occurs. Ensuring security in such settings can be categorised into

several fairly independent areas of identity management: authentication; authorisation; secure communication; auditing and accountability and intrusion detection. For the purposes of the framework presented here we focus on the first two areas namely: authentication and authorisation.

Authentication:
Today emerging grid security efforts are beginning to address application and infrastructure security issues including application protection and node-to node communications. Among other advances, emerging grid security approaches are integrating Kerberos security with PKI/X.509 mechanisms, securing peer connections between network nodes and better protecting grid users and applications from malicious or badly formed code.

Thus far Kerberos [3] has been an early and still viable solution to global identity and authentication in somewhat restricted environments, while PKI [6] identities combined with the Transport Layer Security (TLS) [9] protocol is the solution widely adopted in the Grid.

Grid Security Infrastructure (GSI) in the form of Globus as well as Unicore's security model utilise public key cryptography, specifically public/private keys and X.509 certificates as the basis for creating secure grids; however the authentication mechanisms of both systems differ. While UNICORE signs each part of the job with the user's certificate, which guarantees the integrity of jobs and authenticates the submitting user of a job and therefore enables end-to-end security model, Globus toolkit, uses long-term X.509 certificates to generate a temporary proxy that can act on a user's behalf without requiring user intervention. Once created, the proxy is used to grant or deny access to resources found throughout the grid thus enabling delegation. Because the proxy is used across system, this gives the end user the ability to sign on only once. The proxy expires within a preset amount of time.

In order to provide interoperability between UNICORE and Globus solutions, the GRIP project addressed the following key aspects: translating UNICORE requests for job submission, output retrieval, and status queries to the corresponding Globus constructs and mapping of permanent UNICORE user certificates to temporary Globus proxy certificates.

Within this project these functions were to be implemented without changes to the respective architectures. The result of the project is the development of the Enhanced Target System Interface (ETSI) that enables submitting jobs from Unicore clients to Globus systems and return the results of the computation to the users.

Globus and Unicore are not directly compatible with Kerberos authentication. One emerging grid security effort attempts to sidestep this problem by blending Kerberos infrastructure and X.509 certification. The so-called KX.509, developed at the University of Michigan, is designed to provide a bridge between Kerberos and PKI.

Therefore one can see that the use of a common format credentials with Grid middleware implementations is not yet seamless. Even though majority of the heterogeneous grid middleware implementations are based on the Globus toolkit and most of these implementations utilise X509 certificate extensions to address security and access to the virtual grid resources in the respective grid middleware implementations. Considering EDG and Globus as an exemplar situation, neither of these are interoperable with the other. The best situation today is that the new versions of the middleware ignore the certificate extensions that they do not recognise. Rather there are many different solutions to different parts of the problem. One of the reasons for so many solutions is that authentication is the first critical step to any trusted use of resources. Grid authentication must also interact with user and grid resource authentication requirements; therefore, a single monolithic solution is not feasible. The paradigm of federating authentication from various servers and mapping credentials between a common Grid middleware is the most promising solution as proposed by the FeGIMa project.

Authorisation:
Several research collaboration efforts have addressed the authorisation requirements of distributed computing and collaboration. The requirements vary drastically depending on the application. Authentication systems must be simple for users, access policy should be transparent to the user of resources, easy to set and maintain by the owners of individual resources and site administrators.

In Globus a user proxy requiring access to a resource first determines the identity of the resource proxy for that resource. It then issues a request to the appropriate resource proxy. It is up to a resource proxy to enforce any local authorization requirements. Depending on the nature of the resource and local policy, authorisation is checked and if the request is successful the resource is allocated and a process created on that resource.

The verification requires mapping the user's credentials into a local user id or account name. In a GSI enabled grid, the system receiving the request reads the user's name from the proxy, and then accesses a local file to map the name to a local user.

To avoid creating scores of extra user IDs on different grid systems, administrators can assign users to virtual groups. All users from a particular domain can be mapped to a single, common user ID when accessing a given grid resource. GSI is designed this way to help administrators separate outside users running grid computations from local users in need of local administration and support.

In Unicore security model, certificates serve as grid wide user identifiers, which are mapped to local account at each Unicore site. In addition the site retains full control over the acceptance of users based on the identity of the individual, the distinguished name or other information that might be contained in the certificate. Each site can restrict and limit accessible resources at each target

systems, thus retaining the ultimate control.

One of the main authorisation issues is how to name users in a manner that is meaningful both at the resource site and across the Grid. The adoption of FeGIMa federated identity management will address the solution here.

3 Proposal

3.1 Goals, Requirements and Framework

As Stated in the introduction 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.

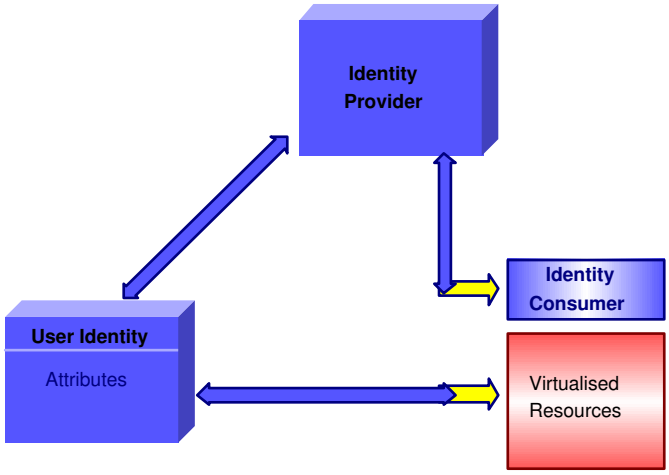

Figure 1: FeGIMa User, Provider, Consumer relationship

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.

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.

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-nymity for protection of personal privacy when assertion of real-world identity is not required or desired.

Overview of Framework:
In designing the FeGIMa framework for the Global ICT infrastructures of the Grid and the Web focus of research will be on three major building blocks (i.e. areas of work), those being:

- Federated Identity Management.
- Trust Management and Policy Execution.
- Intrusion Detection.

In developing the FeGIMa architecture, underpinned from the above three FeGIMa framework building blocks are sub-systems that will be based on the following:

- Base Technologies: will provide the necessary functionality which if missing would render the whole framework ineffective i.e. without the ability of securing communications the goal of privacy is seriously endangered, no matter how powerful the privacy policies, the user is able to define. However these technologies alone are not sufficient to provide an encompassing solution to the problem of federated identity management.
- Core Components: contain the central research targets of the project that will be developed by the consortium partners. These Components are necessary to realise federated identity management in its full scope. They will be integrated with the base components to leverage their functionality, exemplar core components include queries regarding policy or privacy information should be digitally signed and encrypted.
- High-Level Services: are services and applications that will be realised, when the base and core components are developed by the FeGIMa project. They will provide the stage to develop commercially exploitable use cases that will facilitate integrated federated global identity management in the Grid and Web spaces.

To realise the above vision, the project will initially develop the Federated Identity Management component for Grid environments. Subsequently, the integration of the prepared subsystem with already existing Web federated identity systems will be developed. Thus realising the global identity management system. Together with the Trust Management System and the Intrusion Detection System, will compose the integrated Federated Global Identity Management Framework. (see Figure 2)

The realisation of this FeGIMa framework is illustrated in Figure 3: FeGIMa Architecture, illustrating the integration of hither to disparate global ICT infrastructures of the Grid and the Web in an open and adaptive framework that integrates these security mechanisms without endangering the separated and independent grids or the Web. FeGIMa is achieved through a comprehensive security management framework that is extensible and flexible and utilises open standards. The provision of identity information is handled by framework components that employ their respective protocols from the relevant standards allowing for a simplified access to Grid systems or the Web for users.

Next is a selective discussion of the challenges and innovation in the project that focuses on federated identity management within the Global ICT infrastructures of the Grid and the Web.

3.2 Challenges and Innovation

To meet the challenge of federated global identity management through the paradigm of Single Sign On (SSO); thus, reducing the number of separate credentials clearly requires crucial components of strong authentication and credential management. Beyond authentication the need exists to link applications and services, creating persistent and secure sessions to access these applications and services across global ICT infrastructures.

The current state of network identity in the Web requires the user to maintain individual islands of identity where the individual is responsible for remembering the multiple username/password pairs for each of these identity islands, and they must also manage the information that each site maintains in order to ensure that it is both up-to-date and appropriate. Within theGrid the same situation applies to a degree where each grid middleware implementation maintains its own security and identity management system and even where these middleware implementations are based on the same core systems they still do not recognise each other's security credentials. The best that has been achieved as discussed in the state-of-art section of this proposal is the recognition of certificates in middleware that are based on a common implementation (i.e. Globus toolkit, EDG, and NorduGrid) where they ignore each other's certificate extensions or the development of rudimentary bridges (e.g. Globus, Unicore and Grip project).

In addition to the above there exists the problem of user certificate storage, where akin to the identity islands in the Web, certificates are effectively stored in one or more pc's that user utilises to submit jobs to the grid, thereby introducing the weakest link that being the hu-

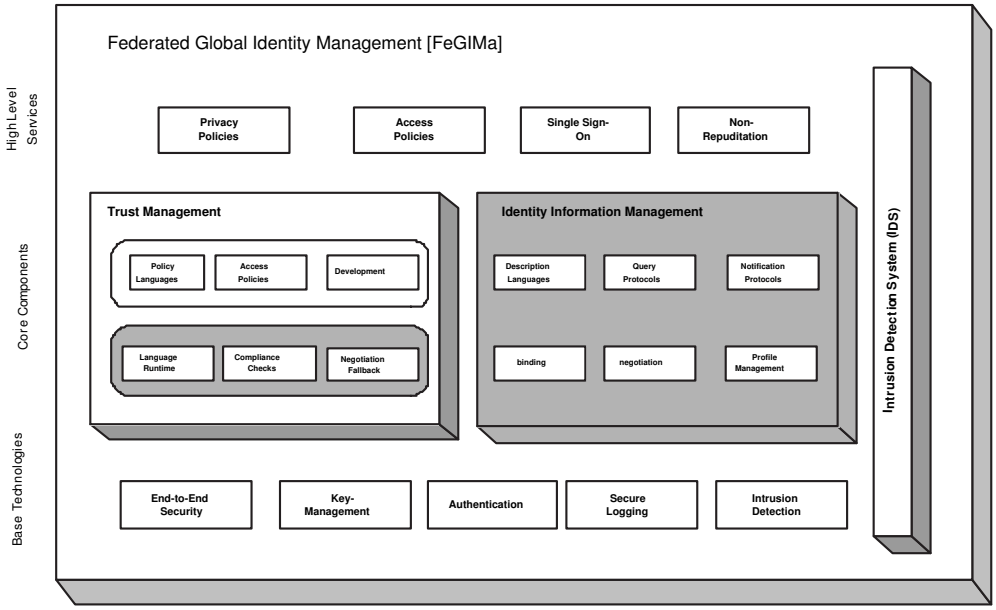

Figure 2: FeGIMa framework

man factor for managing these certificates and ensuring their security.

The proposed FeGIMa Global Federated Identity Management Architecture will address these issues through removing from users the burden of maintaining their identities by providing the trusted hosting service (FeGIMa identity provider (FeGIMa IP)) that will manage the authentication and identification process on behalf of the user (identity owner). The proposed FeGIMa IP will manage authentication and identification process via a number of mechanisms providing weak to strong degree of trust based on the level of service required by the consumer (service provider) in the identification of the user.

The term 'federation' refers to the proposed FeGIMa framework that will make identity and entitlements portable across autonomous policy domains within the global ICT infrastructures of the Web and Grid, thereby overcoming the issues raised consequently federated identity is portable identity "across" these global ICT infrastructures and "within" the same infrastructure. Furthermore, the development of federated relationships between organisations means users (identity owners) have the freedom and the flexibility to move more seamlessly from one service provider (consumer) to another.

The existing approaches of providing security on the middleware layer (Grid) and application layer (Web) deliver intermediate solutions that are not suitable for addressing the needs of roaming mobile users from a user perspective. Furthermore, utilising functionality provided by higher layer services developed by the FeGIMa project will significantly reduce the complexity of interoperable security mechanisms required in the GC Grid infrastructure layer and avoid the co-existence of several independent infrastructures.

The vertical issues of FeGIMa will be based in the analysis of the overall approach with respect to end-to-end attributes, ranging from networking issues until the final orchestration of the services provided to the end-user. Business models that will be applied in the FeGIMa project, will affect all of the layers that are presented in the architecture. It is thus necessary to define all the aspect that are involved in this adaptable configuration for the end-to-end specific attributes of the FeGIMa architecture.

First services are defined on the application support layer providing also an interface towards the user, which is achieved either through direct interaction of offline by means of a contract with a service provider through a Service Level Agreement (SLA). Based on this, negotiation, control and management of the SLA need support for service providers for example as part of a hosting environment and also for a client that needs maybe a service from a different provider that supervises the execution and SLA violations.

Next, the session management and user identity management, which is achieved by the network middleware layer and the introduction of SLA support which will itself require the transference of monitoring and performance information from the underlying networking layer to the Application layer. Clearly, the monitoring and support of the SLA cannot be based on the layered attributes of the current architecture, but it has to be based transparently on the vertical 'signalling' and session management between the subsystems in each layer.

The orchestration of services in the mobile Grid environment implies a vertical approach, since the main aspect that has to be addressed is the adaptation and Configuration of services, resources, access rights (secu-

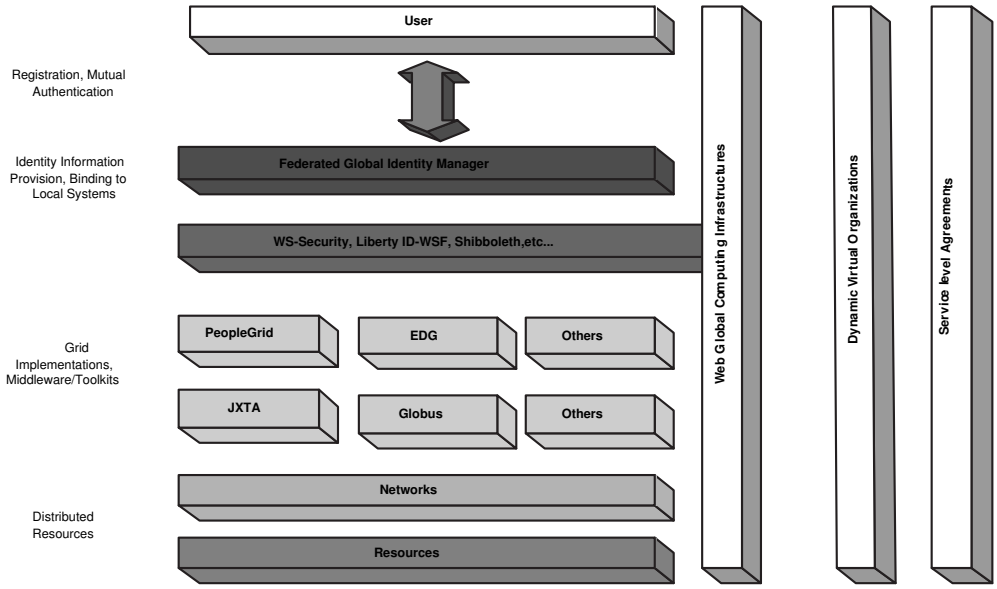

Figure 3: FeGIMa architecture

rity) and networking attributes throughout the various layers of the FeGIMa platform. Orchestration makes essential the use of application-specific functionalities and the adoption of advanced broker schemes to be used for the final synthesis of services. This synthesis is motivated by a session-based approach which will make obvious that the provision of the Application Specific Service to the end user will be subject to a broader configuration management scheme of the underlying modules and submodules. Orchestration and Configuration Management is clearly an essential element of FeGIMa as the enabler of dynamic applications. The usage of orchestrated dynamic applications forms central importance to FeGIMa as it allows adapting the application on changing situations.

Understanding a Virtual Organisation (VO) as an organisational unit bringing together partially the resources offered by different parties clearly poses challenging problems with respect to control, access and the availability of resources provided to the VO's. This issue will be addressed within FeGIMa by establishing an information exchange between the Administrative Domain organisational unit from the Mobile Network Middleware and the Virtual Organisation Management. Where, by means of a user identity model and user identity management framework a dynamic establishment of administrative domains commercially operated by one operator to a VO based on the user-centric needs is addressed. Virtual Organisations having as motivation to provide the means for ubiquitous collaboration among mobile partners will face the need to select the necessary components from every layer in order to perform it efficiently. This is subject not only to the adopted policy for VO management and the selected business models, but also to constraints and/or facts originating from the networking level: wireless hot spots can make use of peer-to-peer computing and ignore access to the legacy networks. One new aspect, which is currently not considered sufficiently in the existing approaches in the grid community is the new requirement, that mobile users as part of the VO might disappear temporarily. For example, a user sitting in a train passes a tunnel and has for 30 seconds no network connection and when leaving the tunnel the same user is connected via a new operator to the same VO. This requires again a coherent management in order to allow the user to continue the session where it was stopped without significant overhead. The FeGIMa architecture will support connectivity seamlessly, which is currently not supported in existing approaches.

The orchestration of Web Services is already moving fast and several competing specification have emerged. Most noticeable the BPEL4WS specification under the auspicious of OASIS, the W3C Choreography Working Group and also the new WS-CAF Framework presented by an industrial consortium. However as Web Services are stateless and the way data is communicated between dependant services on a workflow differs substantially from the needs for Grid Services noted in vertical issues of FeGIMa above. Another issue is the transient nature of Web Services that require the support of on-the-fly instantiation in workflow description languages. Beside the need for notification towards the workflow engine that due to a change of the administrative domain a new set-up is required that is not addressed at all in existing specifications or products. Also during the orchestration process, a close interaction between the network middleware layer down to the network layer is required in order to realise movements of a mobile end-system requesting a service/orchestration process and to adapt in near-real-time to the changing network conditions appropriately.

3.3 Impact

At the highest level the outcome from the FeGIMa project for both sets of stake-holders: 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.

4 Conclusion

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.

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.

Current Internet philosophy does not consider commercial facets. In fact there exists no operational concept to address how roaming agreements and the business relationship between the service providers (network, roaming, Grid Services, Information provided through Grid and Web Services, etc.) and the service consumer with several parties involved in the service provisioning process. Assuming that telecom operators limit themselves through specific service locators the identification process of potential services contract or payment based service access can be established. The service locator could use the user profile provided by his home AAA server in order to identify the services that can be offered to the user in accordance to the creditability and contract the user has with his primary operator. This could be one approach for commercialisation of the value chain from client over the network operator up to the service provider that will be investigated by the consortium.

The explosion of Grid projects and applications worldwide has led to a diversity of approaches. Some Grid computing toolkits are widely used, but none of them has universal acceptance. All of them rely on the standard Internet widely deployed and available almost everywhere. The Internet as it is so far offers only basic transport services and can't offer sophisticated support for fundamental properties of an application middle-ware such as user identification and authorisation or the support for commercial exploitation of offered services.

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.

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".

References

[1] European Data Grid (EDG). (http://eudatagrid.web.cern.ch/eu-datagrid/)

[2] IBM WS Security and Road Map. (http://www-106.ibm.com/developerworks/webservices/library/ws-secmap/)

[3] Kerberos. (http://gost.isi.edu/info/kerberos/)

[4] Liberty Project. (http://www.projectliberty.org)

[5] OASIS, *Security Assertion Markup Language V1.1.* (http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf)

[6] Private Key Infrastructure (PKI). (http://csrc.nist.gov/pki/)

[7] Security Assertion Markup Language (SAML). (http://www.oasis-open.org/specs/index.php#samlv1.1)

[8] Shibboleth. (http://shibboleth.internet2.edu/shib-intro.html)

[9] Transport Layer Security. (http://www.consensus.com/ietf-tls/ietf-tls-home.html)

Mehrdad Naderi graduated with a degree in Electronic Engineering and a Masters degree in Computer Systems specialising in Systems Architecture. He has been for a number of leading to a Software and Systems Development organisations a specialist Systems Architecture consultant r. He was Senior Research Fellow at Sheffield Hallam University, where he was the lead specialist in requirements and systems architecture for the EU IST GRACE project. He researched extensively requirements for Grid Information Retrieval and Security for a Global Computing Platforms and has several publications in these areas.

Jawed Siddiqi is a Professor of Software Engineering at Sheffield Hallam University. He is an internationally recognised Researcher in Software Engineering, particularly requirements engineering. Over two decades, he has served on numerous international committees published over 130 refereed conference and journal papers, has successfully supervised 17 PhD students and currently he is supervising six. He has personally been involved in generating research and knowledge transfer income in excess of G1.5 million pounds. He is an Executive Committee member of the IEEE Technical Council on Software Engineering. He has been a referee for several tenure promotion and professorial candidates in Australia, UK, and the USA. Currently, he serves on the Editorial Boards of the Requirements Engineering Journal and Electronic Journal of e-government.

Babak Akhgar is a Professor of Informatics at Sheffield Hallam University. He has nearly 70 publications in international journals and conferences. He has successfully supervised two PhD students and is currently supervising seven. He has a national and international presence and has often been an invited speaker at EU IST events. He serves on several international programme committees for ICT conferences. He is a member of the prestigious Network Electronic Media (NEM). Currently, he serves on the Editorial Boards of Electronic Journal of e-government and Electronic Journal of Knowledge Management.