IDIS (2009) 2:115–136
DOI 10.1007/s12394-009-0036-0

Federated identity management in mobile dynamic virtual organizations

**Matteo Gaeta · Juergen Jaehnert ·
Kleopatra Konstanteli · Sergio Miranda ·
Pierluigi Ritrovato · Theodora Varvarigou**

Received: 12 January 2009 / Accepted: 27 October 2009 / Published online: 5 December 2009

Abstract Over the past few years, the Virtual Organization (VO) paradigm has been emerging as an ideal solution to support collaboration among globally distributed entities (individuals and/or organizations). However, due to rapid technological and societal changes, there has also been an astonishing growth in technologies and services for mobile users. This has opened up new collaborative scenarios where the same participant can access the VO from different locations and mobility becomes a key issue for users and services. The nomadicity and mobility introduces additional challenges for managing collaboration in VO environments. This paper focuses on the *Identity Management challenge* in a Mobile Dynamic VO environment, which is a VO that takes into account nomadicity and seamless mobility aspects as elaborated within the EU funded project Akogrimo (Access to Knowledge through the Grid in a mobile world). The resulting work is the design of the Akogrimo Identity Management system supporting the authentication and authorization process across the different administrative domains of the Mobile Dynamic VO. This design follows the service oriented approach and integrates the different perspectives: that of the network, that of the user and that of the service provider. Such an integration requires facing challenges; both from the architectural and technological viewpoints because different 'worlds' (i.e. network and service level) leverage different (and sometimes conflicting) approaches when addressing Identity Management.

M. Gaeta · P. Ritrovato (✉)
Centro di RIcerca in Mtematica Pura ed Applicata, Fisciano, Italy
e-mail: ritrovato@crmpa.unisa.it

J. Jaehnert
Rechenzentrum Universität Stuttgart Abteilungsleiter Netze und Kommunikationssysteme, Stuttgart, Germany

K. Konstanteli · T. Varvarigou
ICCS - National Technical University of Athens, Fisciano, Italy

S. Miranda
Dipartimento di Ingegneria dell'Informazione e Matematica Applicata, Fisciano, Italy

Keywords Identity management · Next generation grid · Next generation network · SOA · SSO · Virtual organization · Web services

Abbreviations

A4C	Authentication, authorization, accounting, auditing, and charging
Akogrimo	Access to Knowledge thrOugh the GRId in a Mobile wOrld
AVP	Attribute-value-pair
BVO	Base virtual organization
CD	Customer domain
EAP	Extensible authentication protocol
EMS	Execution management group of services
GSI	Globus security infrastructure
GT4	Globus toolkit 4
ID	Identity document
IdM	Identity management
MDVO	Mobile dynamic virtual organization
MIPv6	Mobile IP version 6
MU	Mobile user
ND	Network provider domain
NGG	Next generation grid
NGN	Next generation network
NP	Network provider
OASIS	Advancing open standard for the information society
OGSA	Open grid service architecture
OpVO	Operative virtual organization
PANA	Protocol for carrying authentication for network access
PM	Policy manager
PR	Participant registry
SA	Service agent
SF	SOAP filter
SLA	Service level agreement
SM	SOAP message
SP	Service provider
SSO	Single sign on
TLS	Transport layer security
UA	User agent
VO	Virtual organization
VOM	VO manager
WS	Web service
WSRF	Web service resource framework

Introduction

Over the past few years, the Virtual Organization (VO) has been emerging as an ideal paradigm to support large scale collaborations among independent, globally distributed entities in order to achieve the VO goal. The enhancement of enabling technologies surrounding the VO vision (such as Web Service (WS), Semantic Web, Grid, utility computing, cloud computing, network technologies) promoted the definition of more ambitious goals aiming at the accomplishment of a unified and integrated infrastructure to share ‘any kind’ of resource (computational, storage facilities, virtual machine, software, etc.) connected through the network.

Several research communities have been working in order to overcome a number of challenges that are obstructing the accomplishment of the VO paradigm.

A critical research issue is related to Identity Management (IdM) spanning across globally distributed administrative domains.

IdM refers to the design of processes and systems that manage and control identities in computer and in telecommunications systems. IdM includes authentication, trust establishment through identity authentication, authorization for access control, exchange of identity attributes, identity lifecycle management, and finally the federation of identities.

Different approaches exist to address the IdM challenge, which can be categorized in the following three main models (FGIdM 2007):

- Isolated: this is the simplest case, where users own a dedicated identifier for each service they access. Although this model simplifies the management of the Service Provider (SP), from the users’ perspective, it becomes difficult to manage as soon as the numbers of identifiers and related credentials increases. Furthermore, processes across several SPs will add a huge administrative overhead generated by the missing convergence.
- Federated: the basic idea is to allow the use of the same identifier in order to be authenticated by a ‘federated’ group of SPs. This means that identifiers valid in different SP domains are linked among them and accepted across multiple SPs. Such an approach is feasible as far as the federated providers trust each other and there is an efficient mechanism to map identities within the SP federation.
- Centralized: this model expects a single identifiers’ provider that is trusted by several SPs. This model decouples the role of service and identifier providers, which can be independent entities.

This paper discusses the design and implementation of a federated IdM architecture for a Mobile Dynamic VO (MDVO) developed in the context of the EU research project Akogrimo (Ako 2004). MDVOs are VOs whose members are able to change locations while provided or consumed services remain available even after temporary loss of reachability, and while running or yet to be initiated workflows adapt to changed conditions, so that MDVOs are characterized by a strong dynamic element with respect to their organizational composition and their business processes (Stiller and Waldburger 2005). Dynamism and mobility are key aspects of a MDVO and they introduce challenging requirements in management of identities spanning across several independent administrative domains.

The basic principles underpinning the Akogrimo IdM system have been introduced in previous articles (Hasan et al. 2007; Kirkham et al. 2005, 2007). Here, we will detail and extend previous work, stepping forward through the presentation of past results in terms of implementation and validation.

The remainder of this paper is as follow: firstly, we present a scenario to clarify the requirements to be met by the IdM architecture together with an overview of the technical background and their related works. Then, we describe the basic concepts (i.e. MDVO and identity model) related to the Akogrimo IdM process and the resulting architecture design. Lastly, we summarize the implementation and validation results.

Motivation

This paper describes the work we have performed within the framework of the research Project Akogrimo, partially funded by the EC under the FP6-IST programme.

The global objectives and visions of Akogrimo were centred on the notion of the 'Next Generation Grid' (NGG), which is usually described by experts in the field as a result of an evolution process comprising three complementary dimensions—namely the end-user perspective, the architecture perspective, and the software perspective (NGGEG 2006). Akogrimo has addressed also the mobility paradigm as a key aspect of NGGs. Pursuing a strict service oriented approach, Akogrimo's NGGs is based on and vertically co-operates with mobility-enabled IPv6 infrastructures and network related middleware.

Figure 1 shows a two-level view of a typical NGG as envisaged in Akogrimo. The upper level is related to the user and service perspective: the Mobile User (MU), belonging to the Customer Domain (CD) that buys services from several SPs, uses such services participating in a common VO (dotted curve in Fig. 1).

The NGG can be understood as a large system of nodes providing added-value services that can be aggregated in an appropriate manner to create new services (e.g. in Fig. 1, the service owned by SP_A is an aggregation of services from SP_C, SP_D, and SP_E.)

The lower level represents the network perspective and it enables the communications using the added value services at the upper level.

The NPs play a central role and they are considered a specific SP case. In fact, they provide the basic services to connect the MU with the added-value service to be consumed.

It is clear that in order to establish an end-to-end communication (from the MU to the final provider), it is necessary to pass across several domains that due to the mobility of the user (and service) could not be known in advance.

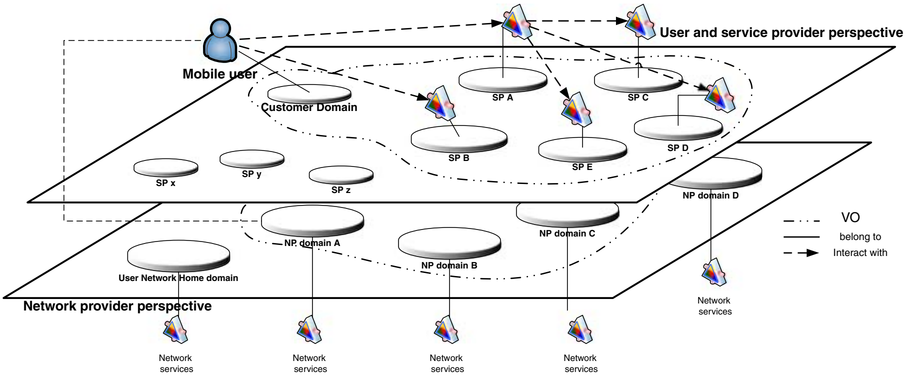

Fig. 1 Interactions in a NGG

This requires an IdM system supporting an integrated Authentication and Authorization (AA) process that allows overcoming the multiplicity of existing mechanisms discouraging resource sharing and collaboration. In particular, such a solution has to address the requirements arising from the different parties involved:

- From the user perspective, the primary requirement is simplicity: access to the resources should not be significantly different from access to a local resource.
- From the perspective of the involved domains, the primary requirement is to maintain full access control on their services even if they trust the assertions provided by the federated parties

Related work

Several solutions related to IdM, based on SOA and Grid, exist in a VO environment. Nevertheless, to the best of our knowledge, an integrated solution that takes into account the different issues arising from a NGG environment is not available. In fact, the analyzed works provide solutions to specific problems but they do not treat user, service and network in a comprehensive way. For example: (Mikkonen and Silander 2006) focuses on porting Liberty alliance concepts to the needs of Grid specific resources; (Butler et al. 2000) describes specific tools implemented in order to integrate Globus Security Infrastructure (GSI) mechanisms into applications to be delivered in VO environments; (Ceccanti et al. 2007) presents a SAML-based service, which is independent from the underlying Grid middleware and can thus be used to offer VO-level authorization functionalities in combination with the most popular Grid middleware. More recent projects have proposed solutions for IdM, in particular, we refer to TrustCom (Trust 2002) and BEinGRID (Being 2006). Though the work performed on these projects strongly focus on message level security and they do not deal with the network dimension integration (that is the focus of this paper), some specific topics (Gaeta et al. 2008; Maierhofer et al. 2006; Chadwick 2006; Chadwick et al. 2006a, b) investigated by them are of interests for a possible integration in our IdM model. This is particularly true for results in (Chadwick et al. 2006a) that deals with use of attributes coming from multiple authorities, while in our approach SP uses the attributes it has generated for its users.

Furthermore, projects like PARSIFAL (Pars 2007) conceptually address also the IdM part, PARSIFAL, in detail however, is conceptually built on top of a currently deployed mobile network, which is conceptually a layer 2 network rather than a next generation IP dominated network infrastructure.

This weakness, in terms of integrated solutions, is confirmed in (FGIdM 2007) as well, which presents an analysis of IdM related use cases in order to identify existing gaps in today solutions. Analyzing from three different perspectives (user, application, networking and architecture) the use cases related to the "Integration of IdM in NGN Architecture" (that is the focus of this paper), and referring to (FRANGN 2007; FGIdM 2007) identifies a set of gaps. The IdM model, presented in this paper, addresses some of these gaps and, in particular, proposes:

1. A shared approach for identity authentication among the involved NGN providers based on the use of A4C and SAML servers. This covers the

identified lack of specification of a common IdM approach to support multiple application/services
2. Linking of identities associated to the same user leveraging on the concepts of principal and digital identities. This addresses the lack of linking among the different identifiers distributed and used in the various components and layers of the NGN
3. An integrated solution among the different functional layer of the architecture. This addresses the need for a coordinated and interoperable solution among the various components of the NGN

Technological background

From a technological viewpoint, the two levels presented in the previous section require the integration of different IdM related technologies. While the upper level focuses on application level interactions and it is implemented by leveraging WS technologies, the lower level is implemented using technologies for IdM related to ND.

In particular, the NP infrastructure leverages the three key building blocks: a). IETF AAA (AAA Arch 2000) relying on the Diameter protocol (Diameter 2003) that supports secure communication based on IPSec (IPSec 1998) and Transport Layer Security (TLS 1999) in intra- and inter-domain scenarios. b). Mobile IPv6 for mobility management (MIPv6 2008) used as the standard network protocol in various 'beyond 3G' activities such as the Daidalos project (Daida 2005). C). SIP (Session Initiation Protocol) (SIP 2002) for session handover and signalling.

Furthermore, as already mentioned, the Akogrimo IdM system is designed according to service oriented principles (OASIS 2006; Rotem 2007) and its implementation is based on the following specifications: WS-Resource (WSRF1 2006) OASIS standard enables and standardises interfaces for stateful WSs. WS-Security (WSS 2004) is a OASIS-Open standard protocol describing how to attach signatures, security tokens, and encryption headers to SOAP messages. WS-Policy (WSP 2007) is now a W3C recommendation describing the capabilities and constraints of the security (and other business) policies on intermediaries and end points.

Lastly, security, at the application level, builds heavily on GT4's GSI (GlobSec 2006), which allows enabling security at both the transport level and the message level.

Akogrimo IdM: basic concepts

The focus on mobility in a VO required the definition of a specific model (the MDVO) by the identification of the involved domains and their role, and by the definition of a suitable Identity Model based on the principal of digital identity concepts in order to decouple concerns among the different domains of the MDVO.

Mobile Dynamic Virtual Organizations

A MDVO represents a specialization of the VO paradigm (a dynamic collection of heterogeneous and distributed resources) characterized by members that can join and/or leave the VO dynamically and that can be nomadic or even mobile. In a

MDVO, the involved resources are owned and controlled by various administrative domains; in particular, the MDVO is characterized by five types of domains: Customer, SP, Network, Base VO (BVO) and Operative VO (OpVO).

Figure 2 shows the high level relations existing between the domains involved in a MDVO. The BVO is a sort of market place built by all potential SPs that have agreed on certain formats, constraints and potentially also base contracts for interaction. SPs advertise their services within the BVO and, through a yellow page-like mechanism, customers identify potential services meeting their requirements. This is the preliminary step for triggering (buy service in Fig. 2) the creation of an OpVO using base services (e.g. discovery, negotiation, ...) situated within the BVO. These services allow combining concrete services by selected SPs ('enact service' in Fig. 2).

The OpVO is the run-time environment for applications that orchestrates services from different SPs that contribute to the achievement of the initial request of the customer.

Once the OpVO is setup, a user can start to access the bought Service. Actually there is not a direct interaction between user and provider (as in Fig. 2) but the end-to-end communication transparently spans across several domains. This requires the definition of a suitable identity model taking into account dynamicity, nomadism and mobility that characterize the MDVO.

It is here, that the NP domain plays a significant role underpinning the MDVO and providing full support to the transparent end-to-end communication (arrows linking user and provider domains in Fig. 2). This is achieved by providing network services in accordance with the service oriented paradigm and leveraging an identity concept that is able to offer SSO-based services comprising WSs as well as network services.

The Akogrimo Identity Model

In Akogrimo, a user identity is the set of information attributable to a person. A user uses the identities in order to communicate with other entities. The attributes of the

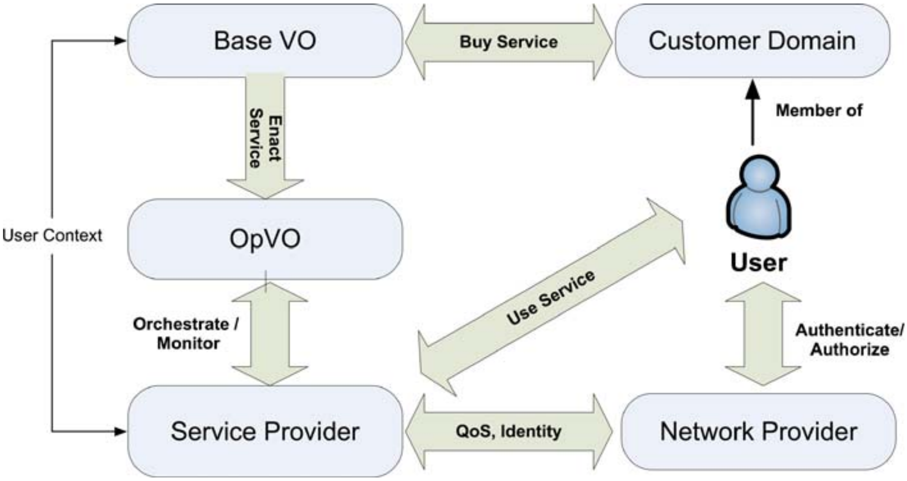

Fig. 2 Relations among administrative domains

users (users identity) are stored either in the home domain or in a SP domain or in the VO domain. Some of these attributes are considered to be of a generic nature and consist of personal user information (e.g. name, sex, age etc.). Other attributes are related to the SP domain of a user and contains information like policies to be applied after a user logs in. The personal user information and home domain specific attributes are stored inside the home domain of a user. A further subset of attributes contains service-specific information. This set of attributes can be stored either in the home domain or in the related domain that provides the service.

In Akogrimo, dynamic representation of a user's identity (within this context the notion identity comprises the attributes assigned to an identity) is foreseen. The detailed representation of the attribute is selected/approved by the user. Within a VO however, policies might require a certain representation. This personalization is performed at the BVO subscription in a very straightforward manner. The identity profiles are stored at the Participant Registry (PR) of the VO to which the user is subscribed. It is foreseen, that the user can act based on various identities, which is conceptually similar to the scenario where different users are acting.

Figure 3 shows the Akogrimo IdM concept from a BVO perspective. When a user subscribes to a BVO, the VO Manager (VOM) adds the user's profile in the PR of the BVO, which is then acknowledged. The key building blocks are the A4C System, the Registry, the BVO Manager and the Admin portal. In the A4C system, a user is represented and all personal attributes are attached to the user. In the Registry, the user is represented as well, but here, SP specific attributes, which should be transparent to the logical function of an Identity Provider are represented. In order to integrate a new user in the VO, a registration in both building blocks is required.

Authorization requests like those from the Policy Management Systems are later sent to the PR and can be answered. Furthermore, A4C servers are statically (within the BVO instantiation phase) configured in a way that they can be seen as a trusted 'community' where new members are not integrated into the communication scenario. By using the standard IETF AAA security mechanisms, all involved A4C (Authentication, Authorization, Auditing, Accounting, Charging) Systems have the ability to dynamically exchange profile information between the PR and Home A4C

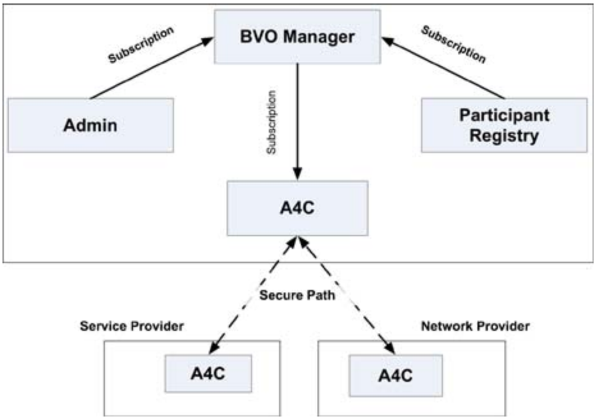

Fig. 3 Akogrimo identity model

Servers—each time, the user's profile changes during his VO membership either at the A4C or at the PR; the other component will be informed about that event by the VOM.

The architecture of the Akogrimo IdM subsystem

Figure 4 shows the Akogrimo IdM subsystem architecture. It is distributed among the MDVO domains and it is centred on the federation of A4C servers hosted in each domain for supporting the authentication process.

While the authentication is managed through a federated process, each domain authorizes the use of its own service according to the attributes associated to the user identity and stored in the domain itself.

The BVO/OpVO infrastructure

Figure 4 shows the components of the IdM system belonging to the BVO/OpVO domain (AkoD443 2006). It is worth noticing that the OpVO is a transient instance of a VO and will need the same components that allow the management of the BVO.

Registries

The Participant Registry (*PR*) provides all manner of information about BVO/OpVO participants. A participant is assigned with an identifier and it is represented using a WS-Resource of the PR that will store information about their status. Each entity living within the VO will have an associated WS-Resource.

Managers

The VO Manager (VOM) interacts as a 'mediator' between the PRs, A4C server, policy manager (PM) and external requestors. All service requests to the BVO/

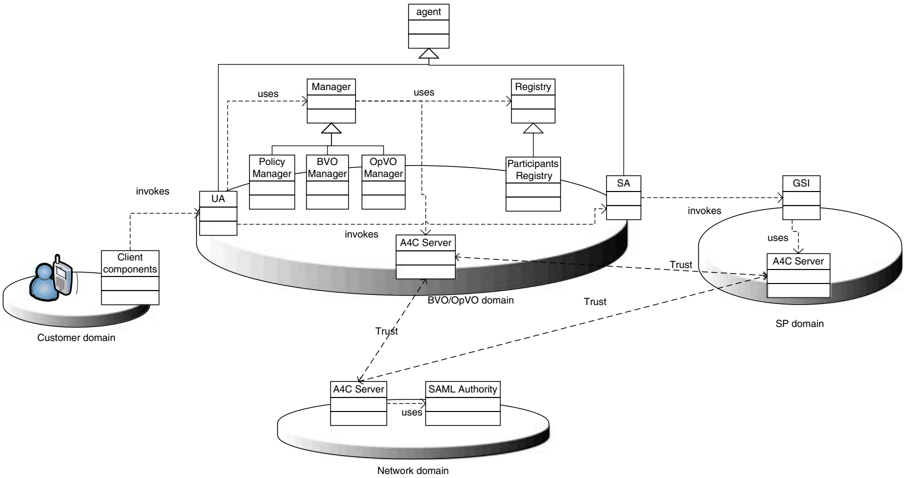

Fig. 4 Akogrimo IdM architecture

OpVO pass through the VOM that requests the A4C to authenticate the requestor through the federated A4C network.

While the authentication is delegated to the A4C, the VOM uses information from the Policy Manager (PM) to make a decision on authorization the request.

The PM presents the VO with a stable set of policies and services organized in a hierarchical tree architecture. The result of a query is an aggregation of policies related to the same subject distributed across the tree.

Agents

The UA/Service Agent (SA) represents the user/service inside the VO. The UA provides a standard front-end to be invoked from the outside and it is the Policy Enforcement Point to control accesses to the BVO/OpVO services. The SA transparently conveys the right credentials to use the respective service in the external SP domain.

The SP infrastructure

The basic role of the SP Infrastructure is to manage the execution of the services on request of the MDVO Infrastructure, aiming to fulfil the Grid requirements, addressing the performance issues in a transparent way to the client and conforming to the determined Service Level Agreement (SLA). The services one can encounter in the Akogrimo SP Infrastructure, apart from the business services that are actually offered to the Akogrimo clients, are listed below:

Execution Management group of services (EMS)

EMS was developed on the basis of the OGSA and WSRF (WSRF2 2004; WSRF1 2006) specifications using Globus Toolkit version 4 (GT4) (Globus 2006). It is therefore responsible for finding execution candidate locations, selecting the one most suitable, as well as, preparing, initiating and monitoring the execution of a business service. Although, from the client's perspective, it appears to be a single Grid service, the EMS is a composition of the six Grid services listed below:

1. *Core service*, which acts as a gateway service that offers a single-point of access to the EMS whilst 'hiding' its details and complexity from the clients.
2. *Advertisement service*, which is used by the SPs to advertise their services in the EMS's index service. The SPs run a client on their local machines, providing all information necessary to form the advertisement of the service.
3. *Negotiation service*, which is responsible for interpreting requests for the negotiation of the terms of the client's SLA contracts.
4. *Reservation service*, which is in charge of performing advance reservation on the resources needed for the execution as well as the monitoring of it.
5. *Discovery service*, which is responsible for finding available services that meet the SLA's QoS parameters. It is designed to follow rules based on low-level performance parameters.
6. *Execution service*, which coordinates the SLA Enforcement and Monitoring group of services and the actual execution of the service.

Monitoring group of services

EMS works closely together with the Monitoring group of services that consists of the following three Grid services:

1. *Metering service*, which maintains run-time information on the performance parameters related to the business service execution.
2. *QoS Broker service*, which is a network broker that handles QoS network requests, and is also responsible for monitoring network parameters.
3. *Monitoring service*, receives notifications about the values of the QoS parameters during execution.

SLA Enforcement group of services

The SLA Enforcement group is composed of the following three Grid services:

1. *SLA-Access service,* which provides access to the SLAs.
2. *SLA-Controller service,* which is responsible for comparing measured QoS parameters against the thresholds defined in the SLA and communicates possible violations to the SLA-Decider service.
3. *SLA-Decider service,* which is responsible for the management of the violations that may occur and decides on the corrective action that should be taken.

More information on their functionality and implementation can be found in (AkoD433 2006; Litke et al. 2008). A high-level overview of services that reside in the Akogrimo SP domain is depicted in Fig. 5.

The Akogrimo authentication & authorization mechanism

The IdM system is designed to reduce as much as possible the end-user intervention.

Figure 6 shows that the end user is initially authenticated by the network (and authorized to access it), then the request passes through the UA and SA within the OpVO domain (the behaviour is similar in the BVO) that authorizes the end-user to use the requested service, finally, the request is forwarded to the actual services in the SP domain that will authorize the OpVO/BVO to access their internal resources in order to satisfy the end user request.

The following subsections will explain in more detail how the different components interact to accomplish the end-to-end communications.

Access to the network

Network access is the first task than is performed in the Akogrimo bootstrap process. During this phase, the user is authenticated by the AAA Server of his ‘home’ domain and an ID token is issued. The authentication performed during network login is based on a username and password and is encapsulated in EAP (Extensible Authentication Protocol) (EAP 1998). For the transport between the mobile end-

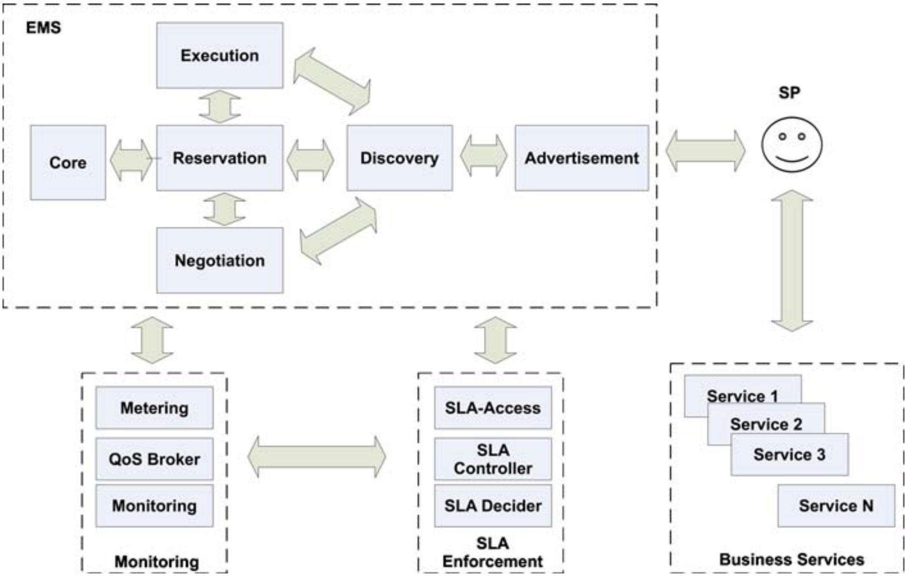

Fig. 5 High-level overview of Akogrimo SP domain

system and the network authentication server, PANA (PANA 2008) is used. For the transport between the network authentication server and the AAA server, the Diameter protocol is used. The following figure shows the network access procedure in detail (Fig. 7).

The mobile terminal (MT) acts as a PANA Client that communicates with the Access Router (AR) via the PANA protocol. The AR communicates with the A4C

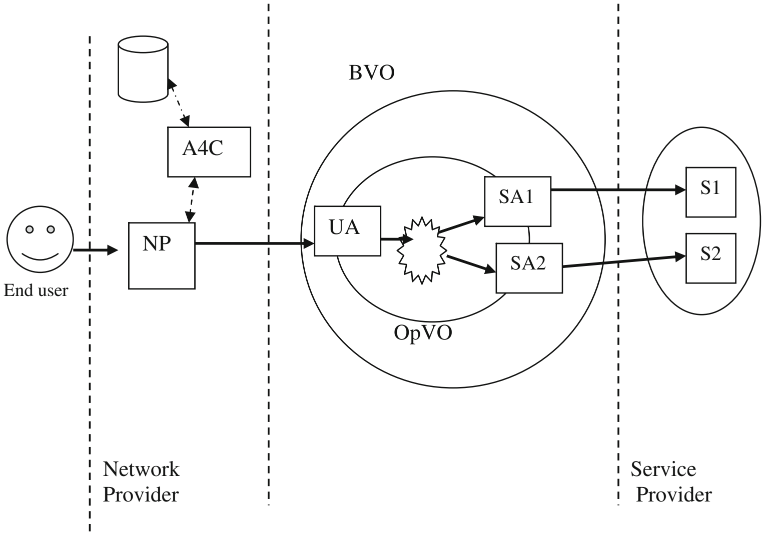

Fig. 6 End user requests across the MDVO domains

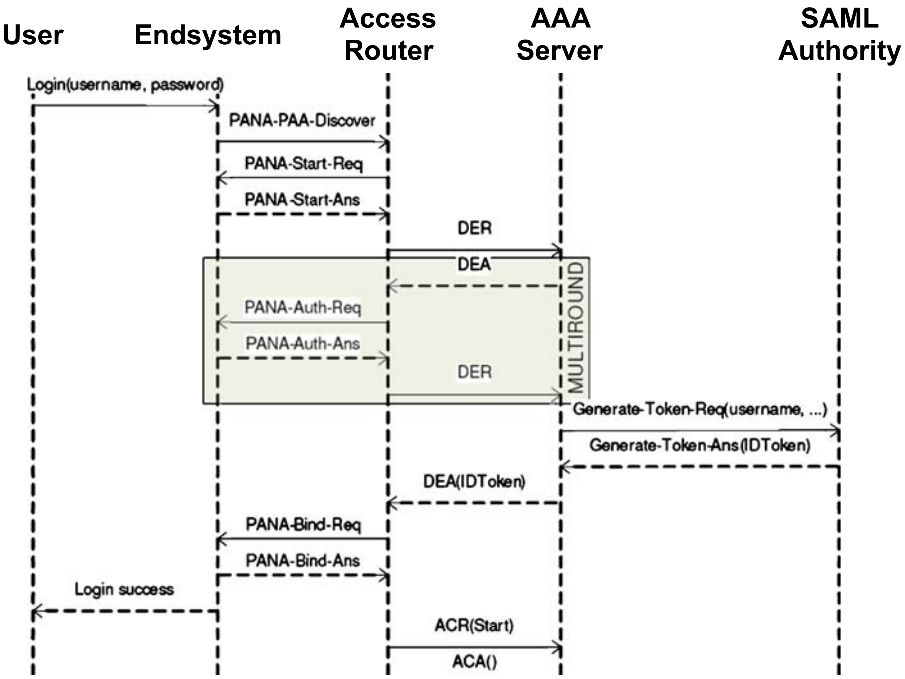

Fig. 7 Network access procedure

server via the Diameter protocol. The communication starts with the PANA-PAA-Discover message sent by the MT to find available ARs. The AR sends a PANA-Start-Request containing information about the network provider. In turn, the MT selects a network provider from the list and sends its selection back to the AR in the PANA-Start-Answer.

The AR forwards the user's identity to the A4C server in the Diameter-EAP-Request (DEAR) message. The A4C server replies with a Diameter-EAP-Answer (DEA). The challenge is forwarded to the MT in the PANA-Auth-Request. The MT replies to the challenge in the PANA-Auth-Request. The AR forwards the message with the answer to the challenge to the A4C server, which verifies the identity of the user.

If the authentication is successful, the A4C server requests the generation of an IDToken from the SAML Authority. Then, the A4C Server sends the IDToken, the user's public identities and VO parameters to the AR encapsulated in the DEA. The information is forwarded to the MT that finally replies with a PANA-Bind-Answer, which closes the authentication process.

Access to the MDVO

Figure 8 shows the AA process related to the invocation of a UA instance.

The SOAP Filter (SF) receives the incoming SOAP message (SM) and parses it to extract the SAMLID token and the claimed digital identity (1). These parameters are passed to the VOM (2).

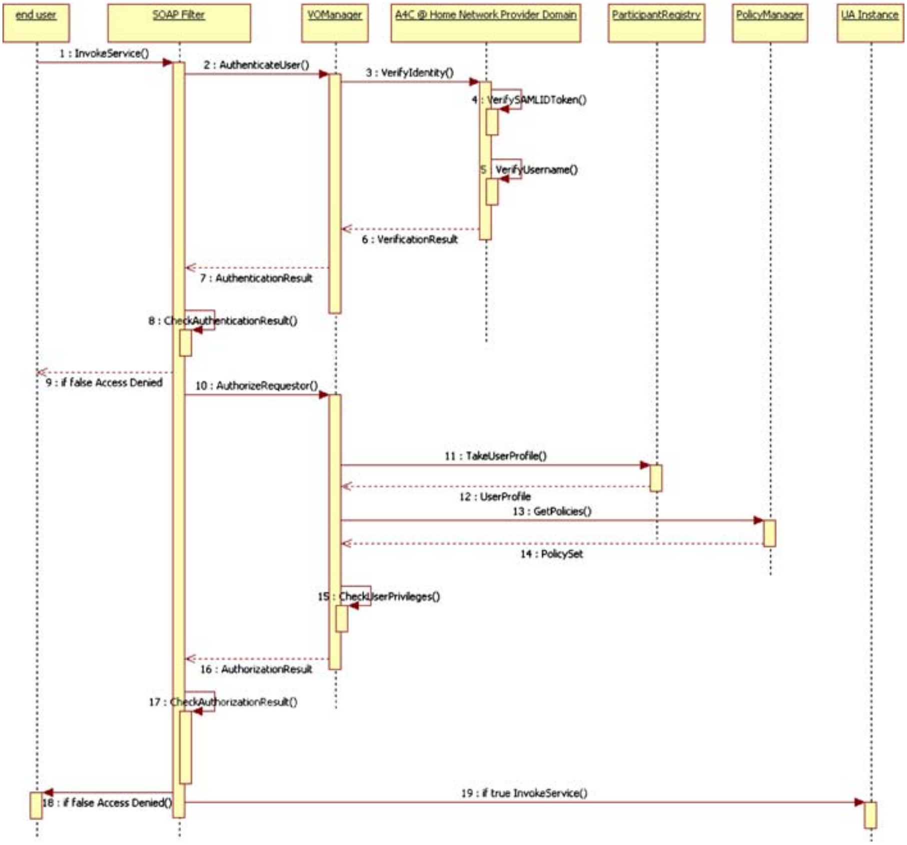

Fig. 8 End user AA

Then, the VOM asks (3) the A4C within the OpVO domain to authenticate the identity. This is done checking the signature of SAMLID token and invoking the trusted A4C server to check the validity of the issued token.

The response (6) of this validation authenticates the principal identity of the user and guarantees that this user is the owner of the claimed digital identity (notice that there is a one-to-many relation between principal identity and digital identity).

The VOM retrieves (11) the profile associated with this identity from the PR and uses such a profile to receive (13) from the Policy Manager the policies (defined using WS-Policy specifications) to be applied for authorizing the request.

According to the decision taken (15) by the VOM, the SF allows the request to be processed by the UA instance (19) or blocks it (18).

Figure 9 shows the AA process between two generic services inside the VO. These interactions are still valid if the generic services are replaced by UA and SA. On creation, these services are associated with a VO token signed by VOM. It is assumed that VOService1 invokes Method() on VOService2.

Figure 9 highlights that the authorization sequence is similar to that shown in Fig. 8, the only difference being the authentication process (2). In fact, in this case, the A4C server is not involved because communications are among entities within

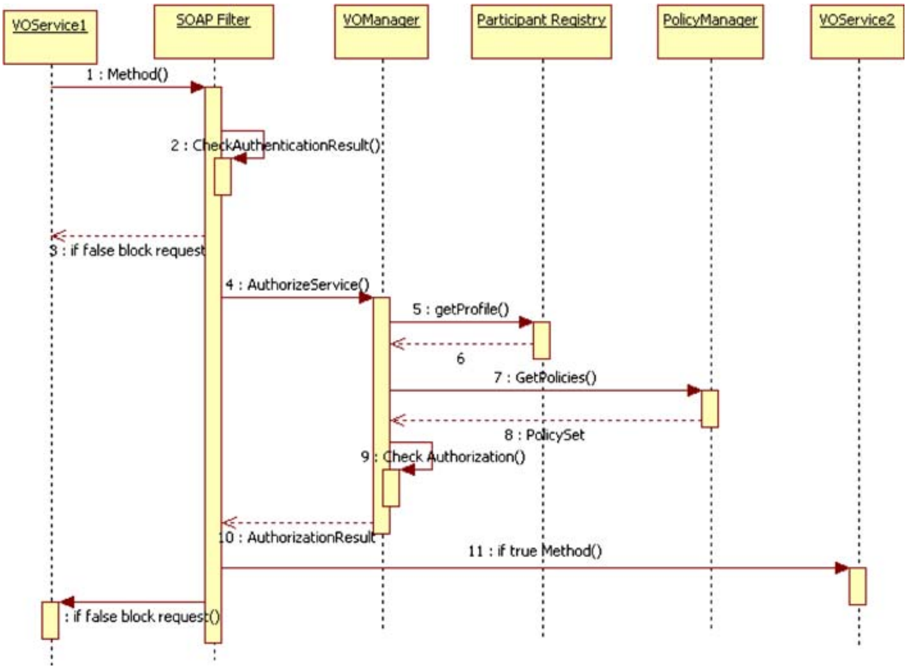

Fig. 9 AA between services inside the VO

the same VO domain and the VOM operates as a certification authority that issues the credentials to be conveyed by the requestors in their messages to be authenticated.

Invoking a service

For the development of the SAs and the SP's Grid Services, two of the most popular platforms in the development of Grid Services were used: GT4 and WSRF.NET (WSRF.NET 2006), both of which are a full implementation of WSRF specifications.

The SA was a WSRF.NET client to the EMS Core service that acted as a gateway service in front of the SP Infrastructure and their communications were made using SOAP over the HTTP protocol. In order to establish secure SOAP communications between the SA and the SP domain, WSRF was linked to the WS-Security specifications and GT4's Security Infrastructure (GSI) was plugged into the Akogrimo security mechanisms.

Authentication

In more detail, the security header of the SOAP request coming from the SAs contained an SAML security token. This SAML token was presented to the EMS Core service. Next, the authentication decision was delegated to the A4C Server that in turn contacted an OGSA-compliant SAML server.

Authorization

Having authenticated against the SAML server, the EMS Core service checked the request against its *gridMap*. If the SA was listed in the gridMap, i.e. the SA was mapped to an account; the EMS Core Service proceeded with the invocation of the specific EMS sub-service. As already explained, the gridMap is used as an access control list. In more detail, during the reservation of the required resources, a persistent WS-Resource was created after each successful reservation inside which all the information that is needed in order to execute the reserved services was stored. For each reservation, an entry was added in the EMS sub-service's gridMap specifying the SA and the WS-resource that corresponded to the reservation. Upon receiving an execution request by an SA, the EMS sub-service checked its own gridMap in order to check if the client that is behind the SA is allowed to access the specific resources in the SP domain. In this way, all EMS services made sure that only the client, who had negotiated and reserved the resources, could actually access them. By doing so, other authenticated clients were prevented from tampering with another client's reserved resources.

It should be noted that the usage and maintenance of gridMap files entries does not scale very well as the number of clients increases. In this direction, the EMS services were able to easily expand onto other nodes in the SP domain to accommodate the increased number of clients. In more detail, when the number of entries in the gridMap file of an EMS service exceeded a threshold, the EMS service was able to delegate its request to another available instance of the same EMS service running on another node or server with fewer clients.

The steps required to invoke a service in terms of authentication-authorization of the SA against the SP domain are depicted in the following sequence diagram (Fig. 10).

Demonstration scenario

The Akogrimo IdM was used in two mission-critical scenarios in public demonstrations. The first scenario was eHealth which focused on heart monitoring whereas the other was in a disaster handling and crisis management (DHCM) scenario in which the eHealth scenario was combined with an overall crisis management. IdM was fundamental in both scenarios since the resources and services that formed the Mobile VO were collected from a wide range of heterogeneous and geographically distributed resources both mobile and non-mobile. Furthermore, the mission critical nature of the scenarios imposed heavy requirements on the performance of the involved services as well as the overall performance of the Akogrimo platform.

The DHCM scenario and the related demonstration are discussed next.

Scenario description

The overall setting of the demonstration is a terrorist attack in the centre of a major city, namely the explosion of a 'dirty bomb'. The management of such situations

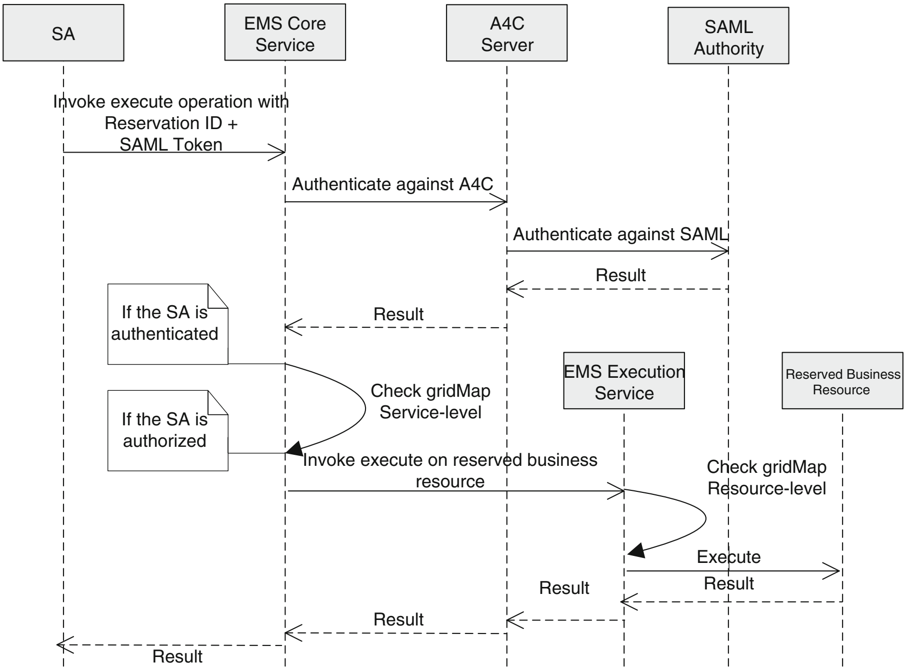
SA
EMS Core Service
A4C Server
SAML Authority
Invoke execute operation with Reservation ID + SAML Token
Authenticate against A4C
Authenticate against SAML
Result
Result
If the SA is authenticated
Check gridMap Service-level
If the SA is authorized
EMS Execution Service
Reserved Business Resource
Invoke execute on reserved business resource
Check gridMap Resource-level
Execute
Result
Result
Result
Result

Fig. 10 Authentication/authorization of SA against SP domain

requires the coordinated collaboration among different entities (paramedic, police officer, fire fighter,...) and the integrated use of different capabilities (camera, video/ audio communication, data evaluation,...). It requires setting up a VO that due to the strong focus on dynamicity and mobility has all the characteristics of a MDVO (see Fig. 11).

The realized prototype is a very rich setting that, with the mobile terminals, networks with quality of service capabilities, vertical context awareness, accounting capabilities, MDVO creation and management, allowed the evaluation of the usability of the Akogrimo IdM model in a simplified real case.

Evaluation results

Having presented the feasibility of the Akogrimo's IdM infrastructure, we present indicative time measurements that have been taken during the demonstrations with respect to its overall performance. Time measurements were performed during the execution phase with security deactivated and activated respectively.

A set of 15 PCs with similar technical characteristics (Pentium V 1.7 GHz, 1 GB of memory, 10 Mb/s Ethernet segment) were used during the demonstrations. All EMS subservices were deployed on the same PC and ran under the same GT4 container. The tests were performed using up to ten different WSRF services that encapsulated the business logic behind the demonstration scenario, developed on the GT4 platform. The Table 1 presents the average response time (in seconds) for authenticating the execution of services where the number of concurrent execution requests bas been equal to 1, 10 and 50.

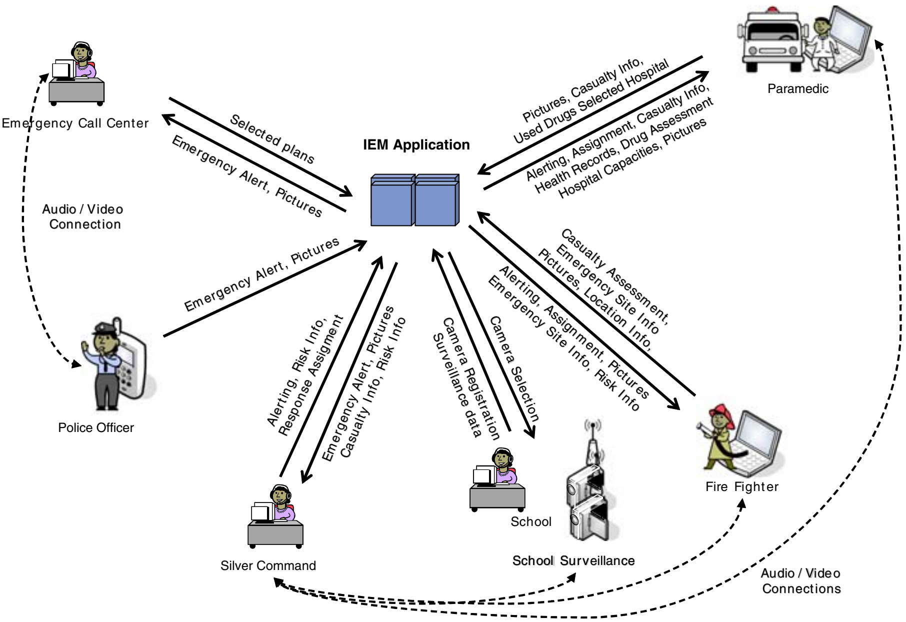
Emergency Call Center
Audio / Video Connection
Police Officer
Selected plans
Emergency Alert, Pictures
IEM Application
Emergency Alert, Pictures
Pictures, Casualty Info, Used Drugs Selected Hospital
Alerting, Assignment, Casualty Info, Health Records, Drug Assessment Hospital Capacities, Pictures
Paramedic
Casualty Assessment, Emergency Site Info Pictures, Location Info,
Alerting, Assignment, Pictures Emergency Site Info, Risk Info
Alerting, Risk Info, Response Assigment
Emergency Alert, Pictures Casualty Info, Risk Info
Camera Registration Surveillance data
Camera Selection
Silver Command
School
School Surveillance
Fire Fighter
Audio / Video Connections

Fig. 11 DHCM demonstrator scenario

where:

T_net elapsed time between receiving an execution request and authenticating against the Akogrimo network

T_mdvo time spent for the process of authentication/authorization against the MDVO

T_sp elapsed time between receiving an execution request by a Agent and authenticating against the Service Provider domain

and consequently:

T_total = T_net + T_mdvo + T_sp total time for authentication and authorization of an execution request against the Akogrimo platform.

Table 1 Results of the experiments (measured in seconds)

Security	# requests	T_net	T_mdvo	T_sp	T_total
Deactivated	1	0.12	0.23	0.45	0.80
	10	2.03	2.97	3.10	8.10
	50	7.40	9.02	11.78	28.02
Activated	1	0.45	1.02	2.45	3.92
	10	3.07	4.56	10.87	18.5
	50	10.34	15.34	25.36	51.04

By comparing the results shown in the table above, some very valuable conclusions can be extracted. As we can see, although it can be considered that the performance scales relatively well as the number of execution requests increases, the Akogrimo IdM adds a significant overhead to the overall performance of the platform during the execution phase. After further investigation, we came to the conclusion that a significant percentage of the added overhead is due to the relatively slow performance of the WS-security related mechanisms against the SP domain. Consequently, as the workload increases, the overall performance of the system might be considered too slow. However, it should be taken into account that the EMS family of services were hosted on the same container which slowed down its performance drastically. Apart from distributing the EMS services across different hosts, another way to improve the overall performance of the system is to introduce new instances of the EMS using a lower threshold for the maximum execution requests as already explained in Section "Invoking a Service". This will allow for delegating the execution requests to other nodes with fewer requests outstanding and will result in a better work-load balancing and improved overall performance.

Implementation issues

The implementation pointed out some issues related to the integration of the involved technologies and the interoperability between the heterogeneous domains.

Due to the requirements for domains' heterogeneity, two of the most popular middleware products were used to develop WSRF-complaint services: Globus Toolkit 4 (GT4) and WSRF .NET. For example, while the EMS and the Monitoring group of services were developed on GT4, all the services in the SLA Enforcement group were developed using the WSRF.NET platform.

It was noticed that, although the WSRF.NET platform is no longer maintained, the presented results are still valuable and up-to-date. In fact:

- The designed architecture is independent of the specific implementation and therefore the proof-of-concepts are still valid even when using alternative technologies.
- Even if the tests were performed using WSRF.NET and the identified solutions are implementation specific, the know-how gained does have a general validity in order to identify the source of interoperability issues independently from the underlying technical implementation.

Integration

The integration issues arise from the need to join the technologies used to secure network and message level protocols in order to distribute authentication information from the network to the VO domain. The component playing the role of interface is the A4C server. In fact, on one side it authenticates MUs accessing the network using network protocols (EAP, PANA, Diameter), whilst on the other side it integrates a SAML authority in order to distribute SAML tokens (used by the MU) and SAML based authentication assertions about the MU that requests services in the MDVO.

The A4C server represents the glue between the network and the VO domain. Again, in fact, it leverages the SAML authority in order to generate assertions understandable at the VO level and makes them available via the WS interface and SOAP standard communications.

Interoperability

At the design level, interoperability among heterogeneous domains is achieved through virtualization of features using the SOA paradigm, implemented with WS technologies. The Akogrimo service-oriented infrastructure allows checking whether the selected popular WSRF development tools, GT4 and WSRF.NET, implement the WSRF and WS-related specifications in a transparent and interoperable way. During the establishment of communications between them, several inconsistencies were detected and were handled in different ways and at different levels with some of them even requiring changing the form of the SOAP messages that were generated by the services.

It should be noted that interoperability problems were encountered not only in the implementation of the WSRF specifications but also in other related specifications that were used such as the WS-BaseNotification specification. Although the WSRF and GT4 services were able to successfully subscribe to one another, problems were detected upon the reception of a WSRF.NET notification message from a GT4 service. Following investigations, the problem was found to be related to the different structure of the SOAP notification message that produced errors during processing by the GT4 related parsers and Java classes. In order to overcome this issue, new classes for processing WSRF.NET notification messages were developed.

A large number of specific tests were also required in order to verify the interoperability between GT4 and WSRF.NET with respect to security management. For this purpose, each service that was used in the tests was configured to use the Platform-specific authentication mechanisms. All tests were made with respect to the X.509 certificates by the OpenCA and each service had obtained a digital certificate from the this CA and used it for authentication purposes by embedding it in the SOAP message using the implementation of the WS-Security, WS-SecureConversation and TLS specifications of the respective WSRF frameworks.

Conclusions

IdM is a challenging problem for management of a large scale VO.

Although a wide variety of solutions have been offered to address the key issues of IdM, the presented work provides a comprehensive view integrating different approaches focusing on two main perspectives: network and service level. In fact, the existing solutions mainly address the problem from a service level viewpoint without providing a unified view of the different parties involved in the service provision in a VO.

The presented IdM system overcomes this weakness providing an integrated design covering all the participants of the MDVO. The initial demonstration proved the functionalities of the implemented prototype, identifying and solving integration and interoperability problems.

These experimental results represent an important step towards extended testing that should evaluate the performance of the developed solution and the potential vulnerability with respect to an identified attack model suitable for the MDVO environment.

Acknowledgements This work has been partially supported by the European Commission under the Information Society Technologies (IST) programme of the 6th Framework Programme for RTD—project Akogrimo, contract IST-004293. The authors want to thank all consortium partners for their fruitful collaboration. This document does not represent the opinion of the European Community, and the European Community is not responsible for any use that might be made of data appearing therein.

References

AAA Arch. Network Working Group. rfc2903. 2000 http://www.ietf.org/rfc/rfc2903.txt. August 2000.

Ako. www.akogrimo.org. 2004. IST-2004-004293.

AkoD433. Akogrimo Deliverable D4.3.3. Report on the Implementation of the Infrastructure Services Layer. 2006.

AkoD443. Akogrimo Deliverable D4.4.3. Report on the implementation of the Application Support Service Layer. 2006.

Being. www.beingrid.eu. 2006. IST-2006-034702.

Butler R, Engert D, Foster I, Tuecke S, Volmer J, Kesselman C, et al. A national-scale authentication infrastructure. IEEE Computer. 2000;33(12):60–6.

Ceccanti A, Ciaschini V, Gianoli A, Stagni F, Venturi V. Virtual organization management across middleware boundaries. Third IEEE International Conference on e-Science and Grid Computing. 2007. doi:10.1109/E-SCIENCE.2007.76.

Chadwick DW: Authorisation using attributes from multiple authorities. In Proceedings of Workshops on Enabling Technologies (WET-ICE 2006), 2006 Winner of Best Paper Award.

Chadwick DW, Otenko S, Nguyen TA. Adding support to XACML for dynamic delegation of authority in multiple domains. In Proc of 10th IFIP TC-6 TC-11 Int Conf, CMS 2006, 67–86, Springer LNCS Volume 4237/2006.

Chadwick DW, Zhao G, Otenko S, Laborde R, Su L, Nguyen TA. Building a modular authorization infrastructure. Concurrency and computation: practice and experience (Special Issue: UK e-Science All Hands Meeting 2006), 20(11):1341–57. ISSN 1532-0626.

Daida. www.ist-daidalos.org. 2005. IST-2005-026943.

Diameter. Network Working group. rfc3588. 2003. http://www.ietf.org/rfc/rfc3588.txt. September 2003.

EAP. Network working group. rfc2284. 1998. http://www.ietf.org/rfc/rfc2284.txt. March 1998.

FGIdM. Focus group identity management. Report on identity management use cases and gap analysis. Report No. 4, International Telecommunication Union—Telecommunication Standardization Sector. 2007.

FRANGN. ITU-T Recommendation Y.2012—functional requirements and architecture of the NGN of release 1. 2007.

Gaeta A, Orciuoli F, Capuano N, Brossard D, Dimitrakos T. A service oriented architecture to support the federation lifecycle management in a secure B2B environment. e-Challenge 2008, Stockholm, Oct. 2008.

GlobSec. Official globus security documentation. The globus security team. 2006. http://www.globus.org/toolkit/docs/4.0/security/.

Globus. Globus Toolkit version 4. The Globus Team. 2006. http://www.globus.org/toolkit/.

Hasan P, Morariu C, Hausheer D, Stiller B. A4C support for commercialization of next generation grid services. 2007. ERCIM News, No. 70. October 2007.

IPsec. Network working group. rfc2401. 1998. http://www.ietf.org/rfc/rfc2401.txt, Novembre 1998.

Kirkham T, Cirillo G, Gallop J, Mac Randal D, Ritchie B, Ritrovato P. An Akogrimo approach to securing virtual organizations within mobile GRID computing environments. 2005. ERCIM News, No. 63. October 2005.

Kirkham T, Lutz D, Movilla J, Mandic P, Gallop J, Morariu C. Identity management in a mobile grid environment. Proc. UK e-Science 2007 All Hands Meeting. Sept 2007.

Litke A, Konstanteli K, Andronikou V, Chatzis S, Varvarigou T. Managing service level agreements in OGSA-based grids. Future Generation Computer Systems Archive. 2008;24(4):245–58.

Maierhofer A, Dimitrakos T, Titkov L, Brossard D. Extendable and adaptive message-level security enforcement framework. Proceedings of the International conference on Networking and Services; 2006, p.72

Mikkonen H, Silander M. Federated identity management for grids. International conference on Networking and Services; 2006. p.69.

MIPv6. Network working group. rfc5268. 2008. http://www.ietf.org/rfc/rfc5268.txt, June 2008.

NGGEG. Next generation GRIDs expert group. Future for European grids: GRIDs and service oriented knowledge utilities. 2006. Report 3, January 2006.

OASIS. OASIS committee. Reference model for service oriented architecture. 2006. Committee Draft 1.0, 2006.

PANA. Network working group. RFC5191. 2008. http://www.ietf.org/rfc/rfc5191.txt, May 2008.

Pars. http://www.parsifal-project.eu/. 2007.

Rotem-Gal-Oz A. SOA patterns. Manning Publication Co. 2007. June.

SIP. Network working group. rfc3261. 2002. http://www.ietf.org/rfc/rfc3261.txt, June 2002.

Stiller B, Waldburger M. Toward the mobile grid: service provisioning in a mobile dynamic virtual organization. 2005. Technical Report—No.2005.7—University of Zurich.

TLS. Network working group. rfc2246. 1999. www.ietf.org/rfc/rfc2246.txt. January 1999.

Trust. http://www.eu-trustcom.com/, IST-2002-2.3.1.9. 2002.

WSP. Web service policy working group. Web Service Policies 1.5—Framework and attachment. W3C. 2007.

WSRF.NET. University of Virginia Computing Group. WSRF.NET v3. University of Virginia. 2006. http://www.cs.virginia.edu/~gsw2c/wsrf.net.html.

WSRF1. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrf, WSRF Specification v1.2. 2006. OASIS.

WSRF2. Web services resource framework. 2004. http://www-106.ibm.com/developerworks/library/ws-resource/.

WSS. WS-Security specification. 1.0. Web Services Security (WSS) TC. 2004. OASIS, January.