

Identity Management in a Mobile Grid Environment

T Kirkham¹, D Lutz², J Movilla³, P Mandic², J Gallop¹, C Morariu⁴

¹ STFC Rutherford Appleton Laboratory, eScience Centre, Fermi Av, Chilton, Oxon

² Rechenzentrum Universitaet Stuttgart, Allmandring 30, D-70550 Stuttgart, Germany

³ Telefónica Investigación y Desarrollo, C/Emilio Vargas 6, 28043, Madrid, Spain

⁴ Communication Systems Group CSG, Department of Informatics IFI, University of Zürich, Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

Abstract: The creation of a secure architecture for a Mobile Grid environment is presented in this paper using conceptual security domains and PKI infrastructure within the context of the Akogrimo EU project. Identity stems from the network domain for mobile services and interacts with the core Grid infrastructure specific services managing the Mobile Dynamic Virtual Organisations (MDVO). A model is presented in this paper where identity sprouts up from the network and policy cascades down from the VO, backed up by SLA (service level agreement) and monitoring services. This paper presents an overview of this infrastructure, how it is applied in current prototypes, the certificate involved and its significance for future development of security in the mobile Grid.

1. Introduction

Akogrimo is a Framework 6 EU project developing a Grid Framework to provide business applications that consist of both mobile services and users. The aim of this framework is to both investigate how the fusion of Grid and mobile technologies to present these applications can be achieved. Central to the challenge of the project is the establishment of seamless linkage and understanding between information presented at both Grid Middleware and Mobile Network level. A key element in the practical establishment of this understanding is within the area of security. Here a mobile Grid has to establish a mechanism by which effective authentication and authorisation for network based services and services existing at the Grid Middleware can work together.

Within Akogrimo this is achieved via the establishment of an intricate identity management system and policy framework. Akogrimo relies on the establishment of Mobile Dynamic Virtual Organisations (MDVO) in the application execution process, these VO's use application specific services that are present only for a short time and are selected during run time. This is achieved through the use of dynamic VO's created from instances of VO's in the base architecture to provide an execution environment for the application specific services. Service selection in this model is based on the premise that mobile services are likely to

change state and replacements may be needed to be selected during the workflow run time.

Therefore the security and policy infrastructure need to work together to ensure that services can be selected and used when representing the right state. This places unique challenges in the creation of a secure environment for all participants in the Akogrimo platform. That is addressed using a conceptual security domain approach supported by a certificate infrastructure.

2. Related Work

Mobile identity management in a Grid infrastructure is a key challenge to the grid research community. In order for services to collaborate the identity of the parties' involved must be known to one and other in concrete terms. The use of mobility presents two main challenges to this in the expression of this identity and transfer of the identity information, as metrics to this differ between nodes at network layer and the grid layer, in Akogrimo they have to cross [1].

In the traditional Grid computing infrastructures identity has been considered as something of a static nature, represented in the form of certificate. In this way, the user and/or the organization present one single certificate with the same identity to all other different organizations, who map the user's identity to a local one representing the user in that specific local organization [4]. This mapping is done with a manually configured Grid map-file. This authentication and authorization is not

appropriate for a Mobile Grid environment where mobility causes frequently changing service characteristics.

Common expression of identity in distributed systems can be seen in the research behind technologies such as the X.509 certificate deployed in traditionally static environments [2]. However for the mobile grid these certificate struggle in the support of mobile identity where a user may need to constantly update the data in the certificate as they move into new environments. For the mobile grid a more flexible and interoperable solution is required, federated identity management has appeared to fill this gap, as a new initiative which intends to include the necessary flexibility and interoperability to support greater user mobility within an identity solution [3, 4]. Further, the federated identity community has realised the importance of the Grid initiative and the need to provide special features not already thought as plain web-based services or stateless web services. This is being addressed with the merger of the Grid and concepts of federated ID emerging in projects such as Shibboleth [5].

Individual identity in distributed computing applications is commonly supporting using PKI frameworks, and this is common to in mobile environments to aid the management of quick reactions to network change [6]... However research into the security of the mobile Grid however can be seen as largely limited to citing the existing research into mobile PKI, or Grid security resulting in the presentation of conceptual architectures [19]. In this paper we introduce a framework that can be used to support secure identity for both mobile users and services in a Grid framework.

3. The Security Domains

The Akogrimo security framework is implemented to support the flow of data in the Akogrimo applications, and to aid its design it can be best visualised as based around four main conceptual domains. These domains are split between the Network Provider (NP), the Base Akogrimo VO, Dynamic / Operative VO, and the Service Provider (SP) domain. The use of these domains underpins the Akogrimo identity management framework. Within each domain there is a local policy enforcement point and certificate verification mechanism. The basic structure and relation between these domains can be seen in Figure 1 below.

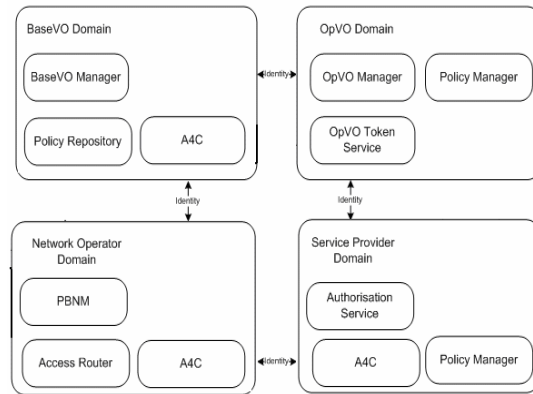


Figure 1: Akogrimo Security domains and Identity.

In the model Network authentication is achieved by the use of an A4C service. The understanding and trust between these services is ensured by a trusted net of A4C Servers that verifies the A4C certificate passed between them.

At VO and Service Provider level the authentication is achieved via the use of specific certificate from the VO and SP domains. These certificates are exchanged prior to application invocation so each domain has knowledge of the certificate that they trust to accept invocations from. In Figure 1 the nature of the credential exchange can be seen as a circular one, and illustrates how the domains are linked in the Akogrimo application invocation process.

The key point in the model from the policy perspective is the BaseVO manager. In order to take part in Akogrimo there is a degree of offline set up which goes beyond the exchange of certificate and registration of credentials with trusted third parties. The use of SLA contracts forms a vital point of the Akogrimo policy foundation, as the service providers and network operators join the framework they agree to the policy terms of the Base VO via the SLA Manager service.

An example how this SLA enforced policy co-operation is achieved is that, by joining the Akogrimo framework, the Service Provider will agree in the SLA that service invocations from the BaseVO which authenticate will be authorised. Thus during run time any local policy that stops this from happening will be solely a SLA issue of service failure to the Base VO and the Service Provider will therefore be liable to any consequence. This will ensure that the external domains working with the Base VO whilst containing there own policy will factor into this Akogrimo use.

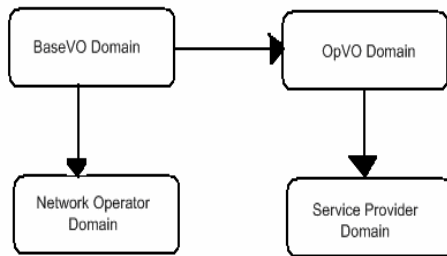


Figure 2: Akogrimo Specific Policy Flow

As Figure 2 illustrates, this policy model produces a hierarchy where policy cascades down from the Base VO to the other domains in the model. Within the VO policy will have a two stringed focus. On an immediate aim the rights and roles of users and services invoking the VO will be handled at either Base VO Manager or OpVO manager level. This will be achieved by the integration of a policy engine such as PERMIS [13] in the two managers, used when a user agent requests an application from the Base VO Manager, or a workflow manager asks for more services from the OpVO Manager.

Policies linked to specific workflows will be installed in the Policy Manager. These policies will be consulted in times of unexpected events outside of the workflows management during application run time. A good example here is Service Level Agreement (SLA) breach (could be caused by service failure). Within the Akogrimo SLA implementation, a SLA Decisor tool exists to contact the Policy Manager for information on the appropriate action to take.

4. Network Originated Identity

Mobile service and user identity in Akogrimo stems from the Network provider domain, where network Identity refers to how an entity is recognized within the network. Users and services use a unique identifier in Akogrimo of the following form: *user@home.domain*, *service@provider.domain* respectively. Next we describe in detail the way identity is implemented in Akogrimo for services in the service provider domain and the VO that can be mobile or not.

4.1 Identity Certificate

The user's identity can only be validated by verifying his Identity Certificate (IDCertificate). The certificates are a small string containing all

relevant data to prove the identity of its holder. In the Akogrimo security approach the IDCertificate can be compared with a user's ID-card. Every time the user has to authenticate, he presents his IDCertificate, which he received during the first authentication step. The use of IDCertificates for user authentication allows provisioning of different levels of anonymity as well as Single Sign-On. The following sections describe in detail how the user obtains the certificate and how it is used to verify his identity.

4.2 Identity Certificate Structure

Akogrimo uses the Security Assertion Markup Language (SAML) [14] to send security information in the form of authentication and attribute assertions to the Akogrimo components. SAML provides an additional security block concerning high confidential information (like authentication and attribute information of a user) in the Akogrimo architecture. SAML is a secure interoperable language used to share user's information from the A4C Server to the other components in order to provide Single Sign-On capability to the user, and to offer attribute sharing of the user to other components.

In order to provide SAML messages, a SAML Engine is needed in Akogrimo, i.e. the SAML Authority. The SAML Authority is part of the security infrastructure in Akogrimo. It generates XML messages based on the SAML standard to send authentication and attribute information. The SAML Authority is an internal subcomponent of the A4C Server. It aims at supplying IDCertificates to the A4C Server. The A4C Server contacts the SAML Authority when it requires to generate IDCertificates and to verify these certificate presented by different components.

The SAML Authority - as part of the A4C Server - is in charge of the generation of the IDCertificate. The IDCertificate is a string containing the following elements:

- SAML Artefact: This parameter is a random-generated number. It is the pointer of the SAML assertions in the SAML Authority's storage.
- Serial Number: This parameter is a counter. It will be increased by 1 each time the IDCertificate is used, in order to avoid replay attacks.
- Random Number: This parameter is a random-generated number and it is

changed each time the Mobile Terminal uses the certificate. It is used to avoid security attacks.

- User Name: This parameter is a string representing the user name of the current user with respect to the User Identifier.
- Signature: The signature of the issuer of the certificate. The IDCertificate is signed by the SAML Authority of the user's Home A4C Server, the first time it issues the IDCertificate, and by the user afterwards.

4.3 IDCertificate usage

The IDCertificate is created from the SAML Authority within the authentication process of the user and it is sent back to the Mobile Terminal when the authentication succeeds, as part of the response of the authentication.

The Mobile Terminal then stores the IDCertificate since it will be needed in subsequent message exchanges with other components. When the Mobile Terminal wants to send an access request to a component, it must first update the IDCertificate, in order to make it secure and valid. This update must be done each time the user wants to reuse it. The update consists of increasing a unit in the serial number and generating a new random number. It then needs to sign the new IDCertificate with user's X.509 certificate, so that the IDCertificate is completely updated.

When a component receives an access request from the Mobile Terminal or any other entity acting on behalf of the user, it receives appended the updated IDCertificate. In order to know if the user is authenticated, it requests the user's Home A4C Server for information of the certificate. The A4C Server then contacts the SAML Authority to validate the certificate and obtain the authentication information in the form of a SAML assertion or to obtain only the information about validation success. The validation of the IDCertificate consists of verification of the SAML artefact, the sequence number and the signature of the IDCertificate. When the certificate is valid, a SAML assertion or a verification statement is issued in order to provide the authentication information of the user. The SAML assertion will contain the name of the user and the authentication method, the verification statement just the username.

5. VO Based Identity

The identifiers for the services in the VO and SP domains have to be compatible for use in each domain. Thus it is logical that they follow the same format. This format will be contained in the certificate which will state the management service name prefixed against the domain name in the certificate that represents the service identity. Thus the level that this is represented at will not be the individual services

An SP certificate contains

- Service Provider Name: hlrs.org
- Service Name: Heart Monitor

A Base VO certificate contains

- Service Provider Name: Emergency Response Base VO
- Service Name: Workflow Manager

An OpVO certificate contains

- Service Provider Name: Emergency Response Base VO
- Service Instance Name: OpVO Number 23
- Service Name: OpVO Manager

These identities will be stored within participant registry services in the respective domains that they are co-operating with, and are implemented using x509 certificate. The reason behind this choice was that the standard is easily interoperable between the two Grid toolkits we are using (Globus and WSRF.net). The use of these certificates and the overall Akogrimo management of identity will now be discussed.

6. Identity Management

Identity management in Akogrimo is made up of two main tasks. The first is identity provisioning and the second application specific role management in the VO. Two important requirements of identity management in a commercial Mobile Grid environment are *Single Sign-On (SSO)* and *Anonymity*. SSO requires that a user should only authenticate once and after that authentication he shall have access to any service he is entitled to use in his home domain or any other domain participating in the Virtual Organization. Anonymity requires that a user should have total control upon the personal information disclosed by his home

domain when the user accesses services of other service providers. The information protected includes (but is not restricted to) the user identifier.

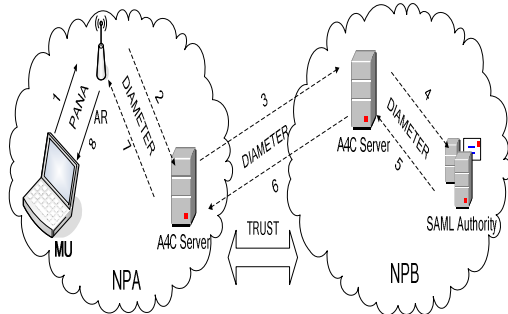


Figure 3: User Authentication

6.1 User Identity Provisioning

User identities are provided and verified by the A4C infrastructure. Before joining a VO user needs to be authenticated. [Figure 3](#) depicts a scenario in which a user (MU) is authenticated even he is not present in his home network. In order for this to be possible, the two network providers (network provider B – NPB – acting as the home domain and network provider A – NPA – acting as the visited domain) need to have a trust agreement. The trust agreement ensures that any authentication done by NPB will be recognized by NPA and vice-versa. During the initial authentication, the user's Mobile Terminal communicates with the access router (AR) to which it is connected to using the PANA [15] protocol.

The PANA protocol is used to transport EAP [16] payloads based on which different authentication mechanisms can be used [TLS/PEAP/SIM/MD5]. The notification mechanism of EAP is used to send back to the user the ID Certificate at the end of a successful authentication. The Diameter [17] protocol is used for transporting the authentication data encapsulated in EAP within a network (from a wireless access point or radio base station to the A4C Server) or across different networks in case of users requesting services from an administrative domain other than the one of his home network operator. If the A4C Server in the home domain of the user (NPB) detects a successful authentication it contacts the SAML authority in the same domain and requests that an authentication assertion is created which is linked to an IDCertificate. The corresponding IDCertificate is then sent back to the Mobile Terminal.

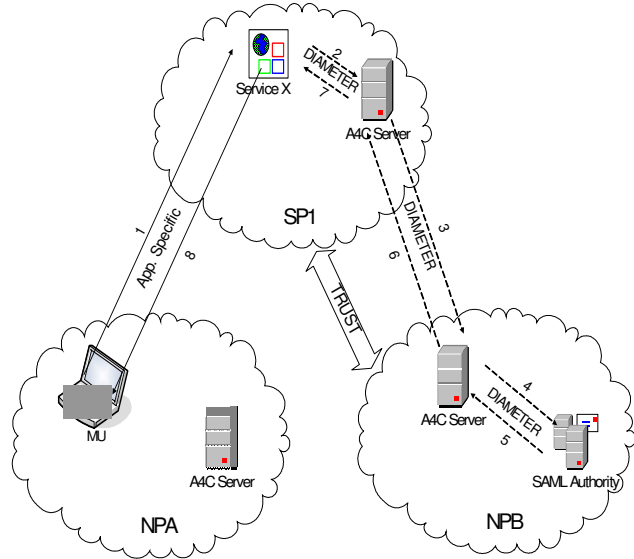


Figure 4: IDCertificate Verification

Once a user received an IDCertificate he may request services offered by the Virtual Organization.

[Figure 4](#) extends the previous scenario so that the mobile user tries to access *Service X* provided by Service Provider 1 (SP1). In the service request the Mobile Terminal shall include the IDCertificate received during the authentication process. Before starting *ServiceX* SP1 needs to check the validity of the IDCertificate and the identity of the user who requested the service.

From the IDCertificate the A4CServer in SP1 extracts the userID and then the home domain that is responsible with the validation of the IDCertificate, and then forwards the IDCertificate to the A4CServer in that domain. For validating the IDCertificate, the A4CServer in the home domain of the user contacts the SAML Authority which generated the IDCertificate. The result of the IDCertificate validation is forwarded to the A4CServer of SP1 together with a profile of the user that also includes the user identity that shall be use by SP1. As the home domain of the user is responsible with the user identity that is announced to SP1, three degrees of anonymity can be achieved:

- No anonymity: The same user identity is always sent to any service provider in which the user requests services.
- Pseudo-anonymity: A virtual identity is created for each foreign domain and always that identity is sent whenever the user accesses a service in that domain.

- Complete anonymity: Each time the user requests a service in a foreign domain a new virtual identity is created.

Thus the identity management structure is built on links between essentially two tiers, the network and middleware. Once the mobile users or services have authenticated via the network specific A4C servers in the Base VO domain, they are issued with a VO certificate, this is used to request specific applications from the Base VO, as the series of events progresses up the architecture.

7. Future Work

The project has demonstrated an emergency response scenario to date with identity provision based on the model above. Future work includes a scenario designed to be more complex involving more actors and examples of mobility changes in the application execution process. However these tests have been more proof of concept and greater detail and examination is needed of the whole model proposed here.

In particular, more work needs to be done in the development of the actual content of the certificate that we distribute in the model, in order to aid more detailed business models and implementations. At the moment, in our initial implementations we only carry basic levels of information related to identity. This level of information will have to be advanced in order to support more intricate levels of policy and SLA management in the Grid.

8. Conclusion

This structure and the management of identity between the network and grid middleware presented in the Akogrimo project is a practical application of security provision in the mobile Grid. The model presents an application where network based security can be scaled into Grid middleware security in a seamless application execution scenario. This is aided by the concept of the four security domains linked to specific network security points represented by A4C servers within the project. This approach is a significant idea, and is practically demonstrated in the projects testbeds where the application relies on seamless and reliable security provision and integration between the network and middleware.

9. References

1. R. Housley, W. Ford, W. Polk and D.Solo "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". IETF RFC2459, January 1999.
2. IETF page Public Key Infrastructure x509. <http://www.ietf.org/html.charters/pkix-charter.html>
3. Federated Identification Management and the Liberty Alliance <http://www.projectliberty.org/>
4. Henri Mikkonen, Mika Silander, "Federated Identity Management for Grids", icns, p.69, International conference on Networking and Services (ICNS'06), 2006
5. Shibboleth project ref <http://shibboleth.internet2.edu/>
6. Kpatcha Bayarou, Matthias Enzmann, Elli Giessler, Michael Haisch, Brian Hunter, Mohammad Ilyas, Sebastian Rohr and Markus Schneider. "Towards Certificate-Based Authentication for Future Mobile Communications" *Journa Of Wireless Personal Communications*
7. Jabeom Gu, Sehyun Park, Ohyoung Song, Jaeil Lee, Jaehoon Nah, Sungwon Sohn "Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications", ISSN 0302-9743, vol. 2727/2003, p.180-191.
8. PERMIS Reference <http://sec.cs.kent.ac.uk/permis/>
9. OASIS SAML webpage <http://www.oasis-open.org/committees/security/>
10. D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin. Protocol for carrying authentication for network access (PANA). Internet Draft (work in progress), Internet Engineering Task Force, July 2003.
11. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz. Extensible Authentication Protocol (EAP). Technical report, IETF, June 2004
12. P. Calhoun, J. Arrko, E. Guttman, G. Zorn, and J. Loughney. Diameter Base Protocol. Technical report, IETF, September 2003
13. PERMIS Reference <http://sec.cs.kent.ac.uk/permis/>
14. OASIS SAML webpage <http://www.oasis-open.org/committees/security/>
15. D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin. Protocol for carrying authentication for network access (PANA). Internet Draft (work in progress), Internet Engineering Task Force, July 2003.

16. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz. Extensible Authentication Protocol (EAP). Technical report, IETF, June 2004
17. P. Calhoun, J. Arrko, E. Guttman, G. Zorn, and J. Loughney. Diameter Base Protocol. Technical report, IETF, September 2003