

AA Developers Meeting

Attendees

Alan Robiette	JISC
Ali Odaci	Alfa&Ariss
Bob Morgan	Internet2
David Chadwick	University of Salford
David Orrell	Athens
Diego Lopez	RedIRIS
Ingrid Melve	UNINETT
Licia Florio	TERENA
Lyn Norris	Athens
Maarten Koopmans	SURFnet
Roland Hedberg	Umeå University
Thomas Lenggenhager	SWITCH
Ton Verschuren	SURFnet
Yuri Demchenko	NLnet Labs

Agenda

1.- Building a inter-operability roadmap: A-Select, Athens, FEIDE, PAPI, PERMIS, Shibboleth, SPOCP

- a) Inter-operability matrix
- b) Requirements
- c) Projects

2.- Open discussion

- a) Protocols. SAML and patent issues. Do we need an alternative?
- b) Attributes. Syntax and semantics definition/publication
- c) Maximizing standardization: authN and authZ APIs
- d) Can we still catch up with Grids?

Introduction

A meeting to discuss about technical details of authentication and/or authorisation software, which have been developing by the academic community in Europe and by Internet 2, was held in TERENA on 15th of April.

Aim of the meeting was the definition of what the different software can perform or cannot, to define a matrix, in order to allow for inter-operability among each other and in some case to complement each other.

The authentication and authorisation systems which were discussed during the meeting were:

- **A-Select**, an Authentication middleware for Web application.
- **Athens**, an Access Management System for controlling access to web based subscription services (<http://www.athensams.net/>)
- **FEIDE**, which aims to establish a common electronic identity for Norwegian academic users (<http://www.feide.no/index.en.html>)
- **PAPI**, which provides support for users to access their information providers outside their network (<http://www.rediris.es/app/papi/index.en.html>)
- **Permis**, a system to implement authorisation on top of existing authentication systems (<http://sec.isi.salford.ac.uk/permis/>)
- **Shibboleth**, a project carried out by MACE/Internet2 to develop policies, structure and architecture to support inter-institutional exchange of Web resources (subjected to access control)
- **SPOCP**, project providing an authorisation engine using S-expressions. (<http://www.umu.se/it/projupp/spocp/>)

1. Building a inter-operability roadmap

Requirements

The meeting started with a quick introduction of all the attendees, followed by a discussion to identify common requirements and define why interoperability is important. Main issues to look for interoperability, a part from sharing code, knowledge and research, are the necessity to avoid several approaches and solutions to common problems, to have a collaborative scientific work environment and to avoid the need of tunnels (VPN, SSL..) when users from one institution try to get authenticated from another institution.

It was agreed that the **authentication** is generally performed at the origin site (the easiest way is through username and password and some agreements to allow users to send these information to their own site), while **authorisation** is performed at the target site.

It was also agreed not to take into consideration, in this stage, how sites manage users, but to consider what attributes need to be exchanged among sites, which want to communicate.

Five different ways to connect different systems were defined and they were grouped in two classes:

A. Local- Proprietary methods

1. Native API/Protocols
2. Underlying server infrastructure(Apache notes/variables; Java environment)

B. External-Standard

- 3. SAML queries/response
- 4. LDAP + trusted objects (this method can use a not secure channel)
- 5. Standard API, such as the GAA API

Roadmap

Diego pointed out four elements to be taken into account to define an interoperability road-map:

- 1. Where are you from (WAYF)
- 2. Authorisation (AuthZ)
- 3. Authentication (AuthN)
- 4. Access control (AC), meant as the actual procedures carried out at the target site once the authorisation stage has been performed. In general, AuthZ procedures can be far more complex than AC. For example, in AuthZ you may want to run SPOCP against a LDAP server or make a SAML query through Shibboleth, while AC may be simply performed by verifying a cookie that was generated at the end of the AuthZ phase.

All attendees were asked to define which of the elements listed above are addressed by their authorisation and authentication infrastructure, which elements each one would be interested in using and how each piece of software would inter-operate with the others. The results are depicted in the picture below.

WAYF Phase 1	AuthN Phase 2	AuthZ Phase 3	AC Phase 4
A-Select			
		PAPI	
		Shibboleth	
		Permis	
		SPOCP	
		Athens	
		FEIDE	

Note: The dashed lines indicate that a function is partially performed; while there is no line in the case that the software does not cover at all one of the phases.

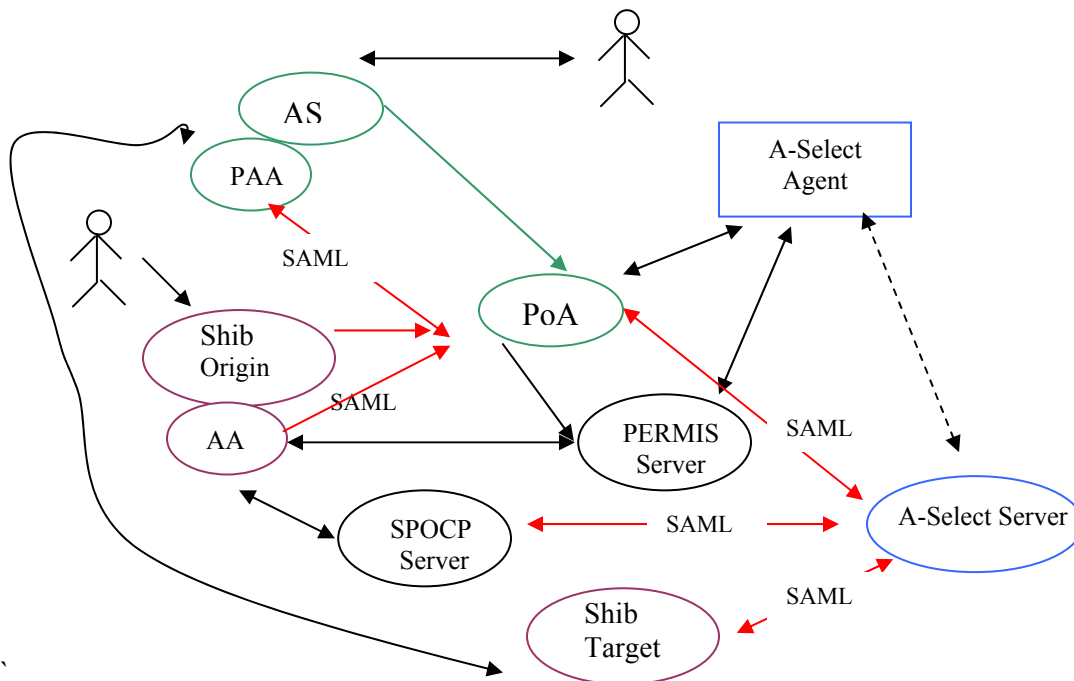
PAPI and Shibboleth only perform partial AuthZ and AC and need additional code to do this.

SWITCH are still working on their authentication and authorisation infrastructure, which will be shibboleth based (for this reason there is no entry for SWITCH in the table). They extended the EduPerson attributes specifications to the switch EduPerson attributes. A running server is expected by the end 2003.

Looking at the previous table the following conclusions were drawn:

- **Athens** is able to perform external authentication and, due to its own characteristics, it could inter-operate with Shibboleth and could trust PAPI, FEIDE and A-Select to perform local authentication.
- **SPOCP**, which can already inter-operate with PAPI, could be complemented by FEIDE and Shibboleth also.
- **Permis**, which is expected to inter-operate with PAPI shortly (a proposal has been prepared by David Chadwick and will be discussed during TNC in Zagreb, in May 2003), do not provide authentication functions; it could inter-operate with Shibboleth.
- **A-Select**, do not perform authorisation. SURFnet would like to inter-operate with SPOCP, Shibboleth and PAPI, using OpenSAML, as depicted in the figure below.
- **FEIDE** could contribute for the attribute generation.
- **PAPI** can use SPOCP for the authorisation and in the future they would like to be inter-operable with Permis, Shibboleth and use FEIDE for the WAYF. The figure below describes how PAPI could talk to Shibboleth.

The next picture describes the how the various pieces can interoperate:



Keys:

———— = PAPI elements

———— = Shibboleth elements

AS = authentication server

PoA = Point of Access

PAA = PAPI Attribute Authority

AA = Attribute Authority

Open Discussion

Security Access Markup Language (SAML)

SAML is an XML-based framework for exchanging security information (such as authentication and authorisation), which is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain.

Due to its definition, SAML provides only a framework and a lot of things related to interoperability are defined by developers. It was also pointed out that the examples are quite few and it is quite hard to figure out how the attributes should be defined, in order to be understood by a Web server administrator.

There was a long discussion about using SAML. It was agreed that the dialect should be avoided and that only OpenSAML should be used.

A proposal, which gathered consensus, was about the definition of a set of SAML rules accepted by everybody. This would be a first step, while the following step would be to verify the rules against each other. The attribute to send to SAML must be precisely specified in order to grant appropriate rights. SURFnet, RedIRIS and Roland Hedberg will work to define such a schema.

PAPI and SPOCP have a SAML interface; Shibboleth, FEIDE. A-Select are moving towards that.

PERMIS currently uses a Java API to interface to its decision engine, but could be modified to provide a SAML interface to a stand alone decision engine server.

Athens is working to interconnect to Shibboleth, so they should be able to talk SAML.

Attributes

Authorisation, which is based on attributes, is complex because the process has to be done on a partnership basis between the subject domain and the resource and the decision is made based on a number of elements. Authorisation systems have a list of attributes that they have to verify against. It was suggested to define which set of attributes can be needed and used, instead than defining and standardising one.

Athens has a simple policy decision and it works on a trusted authentication basis (virtual account details are passed to the service provider), trying to use what the institutions connected to Athens have already in place.

FEIDE works using trusted sources instead than trusted objects.

PAPI, which has been installed in fifteen target sites, is able to use external directories in the setup that RedIRIS is offering to source sites, in order to ease the diffusion of the technology.

A-Select supports a number of back ends for the authentication, so the institutions can choose which method they prefer to use together with A-Select.

Grid

Not very much was said about Grid, apart from mentioning Akenti (an authorisation system somehow similar to PERMIS), and a review of how things are going in the different places. Only UK and Spain are supposed to be trying to link directly Grid and NREN middleware infrastructure. The Internet2 approach seems to be on the style of “absorb and extend”, embracing Grid software in their NMI releases.

Conclusions

The actions defined during the meeting are:

- Lyn Norris will circulate Athens’ technical specifications,
- Roland Hedberg, RedIRIS and SURFnet will work to produce a simple inter-operability document based on SAML, where they will try to learn what actions should be taken to achieve full SAML-based inter-operability