AAI Use-Cases

John White (for the EMI AAI Group)

EMI INFSO-RI-261611
EMI Security Area meeting, Feb 23/24th 2011, Zurich

Introduction

- **Review from AAI workshop**
- **AAI Uses-Cases from Twiki**
- **EGI QA Case**
- **Objectives of this discussion**
  - **Reduce the use-cases from many to few.**
  - **Ideally three or less.**

AAI Workshop

General User Results

- Grid users do not want to handle credentials themselves.
- Grid users would like to obtain X.509 credentials and VOMS attributes from other credentials and vice-versa.
- Projects would like to use federated identities.
- Projects recognize that both national and international identity federations will become more important.
- User identities and actions on a Grid should be protected, anonymized.
- Projects realize that access to the majority of Grid infrastructures requires and will require in the future, X.509 credentials.

More complete report available at:
https://twiki.cern.ch/twiki/pub/EMI/EmiJra1T4Security/

AAI Workshop

"Reactions"

- **Grid users do not want to handle credentials themselves.**
- **Projects would like to use federated identities.**
- **Projects recognize that both national and international identity federations will become more important.**
  - Projects are encouraged to use whatever federated/national identity systems.
  - EMI will interface to or provide a means to obtain credentials transparently.
  - Already SLCS, TCS, (EMI STS in the future) can provide X.509

AAI Workshop

"Reactions"

- **Grid users would like to obtain X.509 credentials and VOMS attribute from other credentials and vice-versa.**
  - Security Token Service (STS), pluggable credential service.
  - Web Service interface. SAML $\rightarrow$ X.509.
  - Others later.

AAI Workshop

"Reactions"

- **Projects realize that access to the majority of Grid infrastructures requires and will require in the future, X.509 credentials.**
  - X.509 + VOMS ACs for the future.
  - Need to get federated (SAML?) attributes for use on infrastructures.
  - VOMS Attributes from Shibboleth (VASH).
  - Service between the IDP and VOMS.
  - Integration to VOMS?.

AAI Uses Cases

- **1. User obtains a X.509 certificate based on an AAI credential**
  - A user has an account in an AAI and wants to access Grid services. For this he needs to obtain a X.509 certificate from which he can generate a proxy.
  - X.509 is short-lived:
    - This use-case is covered by the gLite SLCS service as well as others (?). Adaptions are needed depending on a) the AAI federation, b) CA being used.
  - X.509 is long-lived:
    - There is in our knowledge no package that fulfills this this X.509 issuance process out of the box. The gLite SLCS could be adapted. The Terena Certificate Service provides this functionality - but I have no information whether and how the software is being distributed.

AAI Uses Cases

- **1. User obtains a X.509 certificate based on an AAI credential**
  - Comments
    - (HM): If the generation of a proxy is already mentioned here, should the use case also contain how the AAI users are registered to the VO? CW: added use-case 7.
    - (HM): The SLCS service builds the X.509 DN from the AAI attributes according to its configuration. However, in my opinion we need this "logic" in some other use cases too: see for example use case 4 in this mail. CW: yes - this functionality may be relevant in several use-cases.
    - (HM): How would the portals link an X.509 user to an AAI user (same user, but eg. different browser) otherwise? Or do they have to link them? Or should the portals just support one type of token (or method), and ask service like STS to translate another types to a desired one? CW: In my view the AAI attributes must be used
    - (HM): The implementation used by TCS seems to be: confusa . It is in PHP and it's using SimpleSAMLphp. The "main use case" for it seems to be browser-based, but it also somehow supports OAuth to authorize command-line clients.

AAI Uses Cases

- **2. User obtains a X.509 certificate based on a security token from another domain.**
  - This is basically the same use-case as 1 but in this case the user has a set of credential in non-AAI domain (e.g. kerberos) or simply a username/password (e.g. taken from ldap).
- **Comment**
  - (CW): The EMI proposal specifically mentions obtaining X.509 based on token from Shibboleth-based AAI federations and Kerberos.

AAI Uses Cases

- **3. AAI-enabled portals to Grid infrastructures.**
  - A user accesses an AAI-enabled portal from which he submits grid jobs. The user is not aware that a certificate is obtained based on the SAML assertion from the AAI and this certificate is used to submit commands to the grid.
- **Comment**
  - (HM): Should the use case mention credential stores (like MyProxy), optionally (or not?) in between the portal and the service that issues the certificate? Some users may prefer delegating a proxy to the portal from such a store instead of giving access to the private key corresponding to the "real" certificate.
  - (CW): yes - see below.
  - (CW): The portal may obtain a SAML assertion targeted at another service which then issues the certificate. The portal should generate the private key. It's a question what the portal does with the certificate after that - stores it somewhere else or manages itself. Alternatively, one can also imagine that the portal obtains proxies and the proxy issuing service manages the certificate.

AAI Uses Cases

- **4. AAI-enabled portal for displaying and accessing information about the Grid.**
  - Today, there are many portals in the EGI infrastructure using portals (GOCDB, GGUS, ...) where a certificate in the browser is used for authorization. In theory, all these portals could be AAI-enabled, the question for which (if any) this makes sense.
- **Comment**
  - (HM): To not require client X.509 in the browsers would clearly make the services easier to access from wider scale of devices, "public" computers etc. This would also offer pseudonymity features automatically, of course depending on the attribute set that AAI provides about the users .

AAI Uses Cases

- **5. A Grid service obtains a user-request from another security domain and based on the token obtains a X.509 certificate with which it communicates to other grid services.**
- **Comment**
  - (CW): This needs to be specified in more detail (e.g. for which grid services this could be useful).

AAI Uses Cases

- **6. Use of AAI attributes in Grid services:**
  - AAIs typically authorize the user based on attributes. The question is to what extent are these attributes useful in Grid environment. Example of AAI attributes are:
    1. home organization (i.e. employing institution)
    2. affiliation (student, professor, postdoc)
    3. study branch, study level (physics, 5th semester)
  - Motivation: the matrix of VO vs employing institution provides interesting information on the usage of the Grid, e.g. NGIs can gain information which ones of their constituencies are using the Grid (e.g. for accounting and charging). However, many of the AAI attributes are probably of little value for the Grid.

AAI Uses Cases

- **7. Registration in a VO.**
  - During the registration of the user in a VO, his identity must be vetted. This can be done through AAI. Optionally, a set of AAI attributes can also be involved in this process.

EGI QA Document

ID:	CREDMGMT_LINK_1
Title:	Institutional Authentication Linking (Not Mandatory)
Applicability:	Credential Management Appliances
Summary:	Users should be able to access grid resources using institutional authentication systems.
Technical Input:	Testsuite for linking institutional authentication system with the Credential Management implementation.
Pre-condition:	Valid institutional user credentials, user allowed in the service.
Test:	User requests grid credentials using his/her institutional credentials
Expected Outcome:	Short-lived X.509 credential for used created.
Pass/Fail criteria:	Testsuite is provided and passes for each of the institutional authentication systems supported (e.g. Kerberos, Shibboleth)

EGI QA Documents

https://documents.egi.eu/public/ShowDocument?docid=240