

## TF-AACE

### Deliverable B.2

#### Define the components and protocols to guarantee a harmonized operation of A&A systems

##### Deliverable B2 - The Authentication Component

=====

In the Deliverables list, Delivery B2 is specified as "Define the components and protocols to guarantee a harmonized operation of A&A systems". I believe there is a consensus that the authentication and authorisation services are separate and the main components of an authentication and authorisation service so let us start from there and discuss authentication. (I can't really understand what you mean here; maybe you mean that AuthZ and AuthT are separated and that there is consensus on the fact that authentication should be done at the home institution and that PKI is one of the techniques to provide it ?)

The purpose is not to agree on how to do authentication but on how to describe how authentication can be done.

To move this deliverable forward I will in this message present an initial opinion on what models there are of Authentication Services. Initially at least this discussion will be held on the tf-aace list.

Some Initial Definitions **shall we use for this the AuthZ Grid definitions?**

=====

Identity -- A defined name assigned by an Identity Authority guaranteed to be unique within the Authority's namespace. It may refer to one particular person, process, service, or machine.

Identity is, according to my online-dictionary (Babylon), the "qualities that identify a person or a thing".

Identification is, for example, to pick out Torbjörn Wiberg, using his identity, in a group photo of tf-aace members. (do we need to define this?)

Authentication -- The process by which one party proves to an independent party its right to assert a given Identity.

Authentication is the process of me convincing somebody that I am Torbjörn Wiberg by referring to some qualities of my identity.

I think we should also define here the Authorisation

Authorization -- the process by which the receiver of a request determines whether the request should be permitted

Web Authentication or ...

=====

An authentication service can be a service designed to authenticate users of a web resource or it can be a more general authentication service like Kerberos.

The service can be provided as a library or as a network based infraservice (middleware service).

I would say something more here.

A Web based authentication system is very simple and all the functionalities are located at the edge of the network, where there is installed an access control device to protect the network from unauthorised accesses. When the users get connected to systems, which uses a Web based authorisation they are redirected normally to a Web page, where they are asked to provide their credential (User name and password, normally). Then the access control device will authenticate users against these credentials.

The way the credentials are carried out depends on the implementations.

Federation and Identity

=====

When we come to identity in combination with the concept of a federation, there are at least two different relevant definitions and some variants in the services.

Shibboleth is said to develop system components that facilitates inter-institutional sharing of web resources. On the front page of the web site - <http://shibboleth.internet2.edu/> - it is stated that a key concept is Federated Administration. In the explanation of this notation it is said that a "trust fabric exists between campuses". This trust is manifested by for example the fact that the user's home campus is trusted by the members of the federation to carry out the authentication irrespectively of where in the federation the authentication is requested. So what is carried out perhaps can be said to be Federated Authentication.

The same meaning of the word is used in FEIDE. My unreflected interpretation of the notation is the same as well.

Shibboleth and Feide though differs in that Feide has an internal index service and "knows" which member of the federation that shall authenticate a certain user. In Shibboleth, the user directs the system to the authenticating organisation.

Perhaps you could say that Shibboleth is an Authentication Gateway and Feide is an Authentication Broker.

PAPI also assumes that the authentication shall be done at home by an Authentication Service component. In PAPI a federation of authenticating organisations and access points (PoAs) to content providers is set up. Each authenticated user is attributed with a list of content providers whose resources are available to the user. This list is used by the other system component in PAPI - the PoA - to control the access to the resources of the content providers. As far as I understand PAPI the focus is on the Access Control Component of this federated structure and it can work with different Authentication Services as long as they can include a list of available content resources as a part of their authentication response.

PAPI also assumes that the authentication shall be done at home by some Authentication Service component. Authorization shall happen at the target site, performed by an Authorization component. PAPI also has federation approach where the access points to content providers (PoAs) trust the authenticating organisations to do the authentication properly. As Shibboleth, PAPI has additional requirements on the authentication. Its response shall contain a set of assertions to be used by the authorisation component in PAPI.

And again, Federated Authentication in these contexts is when a federation of organisations share the responsibility to authenticate the members of their community.

The notion of a Federated Network Identity is introduced by Liberty Alliance in the white paper "Introduction to the Liberty Alliance Identity Architecture" and other documents, see ["http://www.projectliberty.org/press/LAP%20Identity%20Architecture%20Whitepaper%20Final.pdf"](http://www.projectliberty.org/press/LAP%20Identity%20Architecture%20Whitepaper%20Final.pdf), revision 1.0, march 2003. It denotes a situation where several identities are linked together in the authentication process. One of the ideas behind this is that the use of the distributed identities shall be controlled by the user, thus giving a better protection of privacy.

The Authentication Service can be provided as a Federated Authentication Service and/or as an Authentication Service for Federated Network Identities.

#### The Authentication Mechanism

=====

In the authentication process, the user presents its authentication data, its credentials, to the authentication service. The authentication data belongs to or is derived from the electronic identity. It can for instance be a username/password, or a piece of data, a challenge encrypted with a private key belonging to the electronic identity, digital certificate, something related to the hardware  
WHAT ELSE CAN IT BE?

The authentication mechanisms match the Username/Password with such pairs in a Username/Password (or rather hashed password) database or decodes the encrypted challenge with the corresponding public key.

Other mechanisms are based on one-time password that are either generated by some device or sent to for instance your mobile phone.

In A-Select the user chooses what authentication mechanism to use from a list of alternatives the system associates you with. To me it makes sense to call such an Authentication Service an Authentication Portal.

## WHAT OTHER MECHANISMS ARE USED?

### Characterisation of the Application

=====

The development of the area has in part been stimulated by the wish from the ISPs to be able to protect the network as a resource from unauthenticated users. That is the network is the application. Much of the IETF work has this focus. This has been a natural starting point but it is important to have an application higher up in the abstraction hierarchy as your model application.

As far as I understand Shibboleth has chosen the problem of serving Content Providers while preserving reasonable user privacy as a major application. They don't trust the application with full information about the user's identity and the application has to trust the Authentication Service follows the rules agreed upon for authentication.

Feide, on the other hand, has chosen trusted internal distributed applications as their first model. You are expected to trust the application with information of Your identity, since the purpose of the application includes keeping and updating information about for instance Your studies.

Another type of application is the small application that, due to the trend that every student and every personnel is becoming a user of our systems, for reasons of efficiency and quality needs to use a central authentication service rather than maintaining one of their own. Many of the typical channels in a personal portal belong to this category.

### Models of an Authentication Service

=====

What then are the different possible models in a taxonomy of authentication services? I see models along the following dimensions, and hope that You can add to the list of dimensions, or have opinions about what constitutes these dimensions.

First there are Authentication Services for different types of applications. The (inter)network itself is the resource, Content Providers, Business Applications, Small Applications, ...

Second there are Web Authentication Services and more general Authentication Services.

Third there are different authentication mechanisms, and there are Authentication Service Portals where you as a user chooses the authentication mechanism to use at this particular occasion.

Fourth there are Federated Authentication Gateways and Authentication Brokers, where in the first case You and in the second case the authentication service chooses which member of the federation shall carry out the authentication.

Fifth there are Authentication Services for Federated Network Identities where the identity is constructed out of distributed identity fragments. (If this is a dimension, it is a dimension of identity types. Is it??)

Sixth, the service can be provided as an Authentication Server Infraprovider, a server providing a network based infraprovider for authentication, or as a library that can be linked with the application.

What points in this space are at all of interest? When I hear presentations of A-select, Shibboleth and Feide's Mellon/Moria I have a feeling that we will eventually arrive at a situation where my (and everybody else's) personal Authentication Service is an Authentication Portal where two of the alternatives are an Authentication Gateway and an Authentication Broker. Most of the time the choice in the Authentication Portal can be made without my guidance since the binding between the model and resource is stored in my profile. But every now and then I arrive at a new resource and I have to register my preferred choice of authentication model for that particular resource.