# Internet 2/Shibboleth and Meteor Requirements

The following notes are based comments made on an August 27, 2001 briefing provided by the University of Wisconsin on WebISO, Internet 2/Shibboleth, and SAML. Charlie Miller of the Rhode Island Higher Education Assistance Authority was asked to list the Meteor requirements that were different from those of Internet 2/Shibboleth. This summarized the subsequent discussion.

## Anonymity

Because of library use, the Internet 2/Shibboleth design satisfies a requirement that the user not be identified to the data source (service provider), but must be authenticated and authorized (by role) to have access. This case arises when a user accesses data, such as professional journals, by does not want the journal publisher to know the identify of the user, but would have authorization to provide the information service This is a requirement not yet identified as needed for the student loan industry.

The Meteor application must know the identify of the person in order to ensure that person only access access to her records or, in the case of a parent or guardian, to records of specific students.

## Initiating Authentication

The Shibboleth model assumes authentication would be initiated by the service provider (data provider in Meteor terminology) requesting authentication. The model of the financial services industry (think of using an ATM card) differs by including the information needed for authentication in the original request for information. In this model, authentication is then done by the information provider.

Meteor resembles a portal in the sense the access provider (such as a college or university) initiates local authentication and then forwards that authentication to the data provider. Generally the data provider "trusts" the access provider's authentication. This is true whether Meteor is installed as a standalone application on a Web page accessing the access providers' authentication service or installed on a portal (such as uPortal) and using the portal's authentication service.

## Level of Identification also know as Level of Authentication or Level of Assurance[1]

A user may have provided only limited information to be issued a logon and password (or

1 As Michael Gettes points out, this refers to the way the person was identified to support authentication, so he prefers the term "Level of Identification." Keith Hazelton relates this to the level of assurance. Because it is an attribute of authentication, some use level of authentication. Ryan Muldoon points out this could also be interpreted as related to a role—and in practice it is—or a function of authorization.

some other credential) or may have provided extensive documentation and appeared in person or the password or PIN may have been sent by mail to implictly confirm name and address. An example would be the difference between a student who obtains a logon for a free course (so there is no credit card, but self-supplied name) and a student who has provided transcripts, communicated with the college by mail, and appeared for a photograph.

Different participants in the Meteor Project have different levels of identification and expect different levels of identification to provide different levels of data access. Level of identification is normative; level required is dependent solely on the data provider.

The capabilities of identifying these different levels to the application are now being included in Shibboleth.

## Multiple Sources of Authentication

A student or financial aid professional may have registered with a number of different Meteor data providers. Those receiving financial aid will have a Department of Education PIN, those with financial aid from multiple sources may have logon and passwords from each of those agencies or firms, and some may have logons to firms, such as banks, that also participate in Meteor and let the bank's PIN be used.

The current Shibboleth design suggests a user will be associated with one organization—the student's college or university. Permitting the student to select the source of authentication could resolve the issue, but could burden others with unnecessary steps in logging on.

Often, in the Meteor design, the user will be authenticating using a third-party authentication service; a service that is neither the local portal or web-server or the provider of the information service (data provider).

## Step-Up Authentication

If the level of identification of a Meteor user is less than the level required by a data provider, Meteor will provide the opportunity for the user to logon to another authentication service to achieve a higher level of identification. This "step-up" authentication is not explicitly included in the Shibboleth design.

## Authenticating Broadcasts

There are Meteor requests where a broadcast is done simultaneously to several different potential data providers. To be efficient, the authorizing credential needs to be sent with the request message. This implies that each of the participants know the other is within the "trusted network."