Guest Affiliate Problem Statement (Working Document)

EDUCAUSE IAM Tools & Effective Practices Document: Guest Affiliate Problem Statement Version: 20110515 Category: Informational	Brendan Bellina Mgr, Identity Management Identity Services Architect USC ITS
Comments to: author or IAM-TOOLKIT@LISTSERV.EDUCAUSE.EDU	May 15, 2011

Abstract

This document describes the challenges institutions face providing access to electronic resources to individuals who have a relationship with the institution other than traditional employment or enrollment.

1 Introduction

Institutions of learning often have the need to allow individuals outside of the traditional employment and enrollment relationships to access electronic services. This document describes the problem and defines some of the characteristics of guests and the methods used to grant then access to electronic services and systems.

2 Conventions used in this document

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC-2119.

3 Terminology

authentication (***authN***)

Authentication is the process of establishing whether or not a real-world subject is who or what its identifier says it is. Identity can be proven by: Something you know, like a password; Something you have, as with smart-cards, challenge-response mechanisms, or public-key certificates; Something you are, as with positive photo identification, fingerprints, and biometrics. (For more on this topic, see the Internet-2 Middleware Authentication website at <http://middleware.internet2.edu/core/authentication.html>.)

authorization (***authZ***)

The determination that a request can be honored is known as authorization. (For more on this topic, see the Internet-2 Middleware Authorization website at <http://middleware.internet2.edu/core/authorization.html>.)

4 The Guest Affiliate Problem

4.1 Overview

Institutions of learning often have the need to allow individuals outside of the traditional employment and enrollment relationships to access electronic services. The relationships of these individuals can vary greatly from the highly ephemeral such as a person visiting campus for the first and possibly only time to the virtually permanent relationships of emeriti faculty and affiliated organization employees. Such relationships can rarely be defined by simple life cycles. In some cases these institutional guests/affiliates/associates may have nearly the same privileges as employees, but software and resource licensing agreements may not include this potentially large population and they are treated more as *personae non gratae* than privileged members of the institution community.

Because of the wide variance in potential use cases for this problem, this document describes a framework within which such use cases can be described.

Within this paper the term “hosted institution” refers to the institution hosting the service the guest is accessing. If a guest is a member at another institution, then that institution is referred to as the guest’s “home institution”.

4.2 A Guest Affiliate Framework

It is difficult to clearly identify the distinct characteristics that separate guests from members of an institution. The guests themselves may not be aware that their status is different in any way than that of an employee. No single characteristic is sufficient or required to distinguish guests from members. In general however guests do differ in how their identity information is managed and the establishment of their authorization to resources and privileges in systems.

4.2.1 Characteristics of Guests

The guest's identity information is not collected or vetted through the admission or hiring processes of the host institution.

The guest may be a former member of the host institution whose data and privileges may not be maintained by the same departments that manage current students and employees.

The guest may need or be allowed to access a more restrictive set of services than is generally available to enrolled or employed members.

The guest may be physically remote and never actually present at the institution. This can complicate identity verification.

Guests typically have different life cycles than enrolled or employed members. They may have a short duration and automatic termination by date, and/or may be tied to a sponsor (a regular member or a department) and be terminated if the sponsor loses membership.

A Guest account may be requested using inadequate, self-asserted, and/or fictional identifying information, making vetting difficult or meaningless.

Guests may transition to enrolled or employed members, raising the question of whether to attempt to "convert" the digital identity or issue a second identity.

4.2.2 Methods for Providing Access to Services

4.2.2.1 Provide services without requiring user credentials

It is not uncommon for electronic services to be made available based on information other than a user authentication/authorization event. Common uses include open wireless networks and access to external services based on IP address.

4.2.2.1.1 Open wireless networks

Open wireless networks alleviate the need for individuals to be granted the right to register their computer on the wireless network. This is usually done for the convenience of the guest (and sometimes members as well), although it makes security very difficult to ensure. Unregistered machines on the network that are compromised by viruses and malware may infect other machines and the machine owner may not be able to be contacted.

Institutions that allow open wireless networks for guests may also provide a separate secured wireless network that members are encouraged to use. However as long as an open wireless network is available it will be difficult to enforce the use of a secure network by members.

4.2.2.1.2 Restriction based on network IP address

To prevent the need for members to have accounts at hosted vendor sites resource providers have sometimes allowed access to services based solely on the network IP address of the network device used to access the resource. This assumes that all authorized users and only authorized users are within the approved IP space. This model is easily extended to guests who are physically located at the institution and can be extended to remote guests (and remote members) through the use of VPN (virtual private network) software, which allows devices outside of the institution IP space to be assigned IP addresses within the space, such as home computers.

This approach, although time honored and not uncommon, is inherently risky to both the service provider and the institution. Unauthenticated access to the service allows individuals to use the service in unapproved and untraceable ways. VPN software allows users of compromised devices through the institution's electronic defenses, such as an institutional firewall, and may lead to the compromising of trusted machines and risk to institutional resources and data.

4.2.2.2 Administratively granted service-specific account

Perhaps the oldest method of granting access to services to guests is still the most widely used. Access to an application system or electronic service often requires only a user account and a password. Prior to the implementation of institution single sign-on systems many application systems managed their own user and password database along with their own login service. Providing access to a guest therefore required only an administrator to establish a user record and password in the application database.

Disadvantages of this approach include:

- Application specific accounts can lead to unsatisfactory user experience - multiple passwords and multiple identifiers when requiring access to multiple services

- Manual administration can lead to slow on-boarding and delayed off-boarding processes, increasing user dissatisfaction and security risk

- Potential of inconsistent user data entered into systems

- Creates problematic transition use cases when the guest later becomes a student or an employee of the institution

- Password management likely to be insecure or rely upon known shared secrets such as date of birth and social security number. This personally identifiable information may be stored in the application database which is a significant risk if the database is compromised.

- Relies on the security of the application (password strength, change frequency, etc.)

Advantages of this approach include:

- Restricts access to particular applications which reduces risk of the account being used to access other systems and data

- Departments can provide guests access to department hosted services without requiring involvement of central authorities

- Tends to require very little red tape

4.2.2.3 Enterprise identity and/or account maintained at the host institution

Defining a guest's identity/account within the enterprise identity system of the host institution provides benefits to both the institution and the guest. For the institution this solution leverages their existing Identity Management and security infrastructure, reducing the risk of abuse. It also allows the guest to be recognized, possibly via institution provided email address, as a contributing guest of the institution and work done by the guest reflects the institution. For the guest it helps to ensure a common user experience and identity information is properly shared across multiple services and potentially gives them a way to publicly express their relation to the institution.

Because the identity information collected about the guest may be shared across the enterprise and the guest given access to multiple services, it is not uncommon for guests to require sponsorship by an existing member of the institution. This may be managed by a central organization, delegated to departments, or even delegated to specific relations of the guest – such as allowing students to sponsor their parents and guardians.

Sponsorship however can introduce inconvenience and lead to delays in on-boarding, so some institutions choose to eschew sponsorship and allow guests to self-register. This works best when guests are limited to applications and services that do not require a high level of identity assurance.

One disadvantage of this approach is that the host institution does have to manage the identity data and credential of the guest, and so when that information changes or the guest's association with their home institution changes the information and access privileges may not be updated accordingly.

4.2.2.4 Trust Model with Guest's Home Institution

In cases in which a guest has credentials at a home institution, does not require or benefit from host institutional branding such as an email address, and whose status as a guest is dependent on their active status at their home institution, extending trust from the host institution to the home institution may provide a more secure alternative to the guest problem. Mature standards-based Single-Sign-On systems such as Shibboleth are capable of using the SAML (Secure Access Markup Language) protocol to exchange attributes between host and home institutions so that the guest can login at their home institution using their home institution credentials and then be given access the services at a host institution. This prevents the host institution from needing to create or maintain credentials for the guest and also reduces the need for sensitive identity information about the guest to be stored at the host institution. In this scenario the home institution acts as a trusted identity provider.

The trust with the home institution provides both advantages and disadvantages:

- The home institution controls the attributes that are provided about the guest to the host institution. This works well when the home institution's account practices ensure that the guest is recognizable persistently and that no two guests can be mistaken for being the same person. This requires that the home institution release persistent unique identifiers for each guest that are never recycled. If not, then the host services may be at risk of current guests accessing the information of former guests.

- The home institution controls the authentication event. The home institutions account practices will determine whether the user account can be used to access the hosted services. The home institution may have very different account practices and security protocols in place than the host institution, which could put the host institution at risk.

- The home institution may not communicate with the host institution when someone has left their institution. While access to the service may end because of the home institution account being disabled, the host institution will not know that data created by the guest can be de-provisioned.

- Because the home institution is providing the authentication, it is easy to assume that this indicates a degree of trust is warranted and so sponsorship may not be required. This may be a dangerous assumption to make without understanding the practices of the home institution regarding accounts and guests.

4.2.2.5 Trust Model with Federation

This scenario is similar to the trust between a host institution and a guest's home institution, except that the trust is extended to a federation (or web of trust) rather than individual home institutions. This allows guests from a variety of institutions access to the hosted services minimizing the set up time for each institution. This scenario bears the same risks that establishing trusts with many individual home institutions would have. There is increased risk if the host institution chooses to blindly trust any federation member's access by default.

4.2.2.6 Trust Model with Social Networks and User-centric Identity

With the growth of Social Networks such as Google, Facebook, and Twitter and user-centric identity solutions such as OpenID, it is increasingly likely that a guest of an institution has credentials provided by a social networking site. As with guests who have home institutions, if there is no benefit in branding the guest with a host institution identifier, and if the service being accessed does not require a high level of assurance, then it may be reasonable to allow the guest to use their social network authentication and identity to access the hosted service. This is a solution that schools are just beginning to experiment with.

5 Links

Access Management Use Cases Organized by Area of Interest (CAMP 2009)

OpenID Use Cases (Social and Organizational Discussion Space - Internet2 Wiki)

6 Change Log

This section lists the changes (other than typographical corrections) that have been made between released versions

20110515.01 Initial internal release (draft)

20110518.01 Added additional guest characteristics to section 2.4.1 per David Bantz (Mark Scheible)

7 Contact Information

EDUCAUSE IAM Tools & Effective Practices working group

Email: IAM-TOOLKIT@LISTSERV.EDUCAUSE.EDU

Brendan Bellina

University of Southern California

Email: bbellina@usc.edu