Guest-Affiliate System Self-Assessment

(PDF document of Assessment)

Introduction

This document is a draft of a self-assessment tool to help campus IAM architects (and others) determine how best to provide access to campus services for guests and other affiliates who do not have a campus credential. Users of this tool should also refer to the companion document "Guest Affiliate Problem Statement" (also a working document) for a better understanding of the Guest Affiliate problem. The sections of the assessment are divided into three parts: policy, business practices and technical.

Term Definitions (for this document)

- Member - implying that the individual's affiliation to the institution is Student, Faculty or Staff (active)
- Guest/Affiliate - used interchangeably in most cases, however, primary distinction is that they are NOT members. (Guest can have a shorter-term or less frequent association, versus affiliate which could be longer-term or a lifetime affiliation such as Alumni).
- Campus Credential - a username or digital certificate issued to members of the institution (e.g. a NetID).
- Guest Credential - a username that is distinct from a Campus Credential.

Scoping Questions

- What are the use cases for the creation of a Guest/Affiliate System?
- Do you require a System of Record (separate data store) for Guests/Affiliates? (e.g. NOT in HR or Student systems)
- Do you intend to use a separate authentication mechanism/system for Guests/Affiliates?
- Do you intend to create a separate Guest Credential distinguishable from a Campus Credential?
- Will some of your services, applications, resources be accessible by both Guests and Members? If so, will both Guest and Campus Credentials be used or will guests that need to access these services be issued a Campus Credential?
- Is it possible for some individuals to have both a Campus and a Guest Credential?
- If you intend to have separate credentials (those for Guests and those for Members or "special" guests), will you TRANSITION individuals between the authentication systems if they are separate?

Policy

Self-Assessment Questions

- Do you have a policy that clearly states eligibility requirements for guest accounts and access to services?
- Do you have a policy that clearly states the approved on-boarding processes for guests? e.g. self-service, department designee, central request-approval workflow, etc.
- Do you have a policy that states who may sponsor guests?
- Do you require term-limits for individuals acting as sponsors?
- Must a sponsor renew the ability to sponsor accounts?
- Do you have a policy that clearly states which data can be used to verify (vet) the identity of a guest?
- Have you clearly stated any limits on how long a guest account can remain active (authentication enabled) before being terminated, reviewed or renewed?
- Have you clearly stated how long guest identities are to be retained in your system?
- Have you defined the minimum set of guest attributes that need to be captured? (Required for matching and merging - deduping against existing guest or member accounts)
- Do you require attributes to indicate the identity is a guest, who the sponsor is, when the account expires, etc.?
- Have you clearly stated any restrictions on applying affiliation attributes (e.g. faculty, student) to guest identities, especially on standard attributes like eduPersonAffiliation?
- Have you documented and communicated who is responsible for supporting guest identities -- your central help desk or a special guest help desk?
- Do you allow individual service providers to decide which, if any, guest credentials they will accept? Have you clearly documented any rules they must follow? Will this require the creation and approval of new or additional attributes?
- Have you stated whether guest credentials can be used to access any/all external services (e.g. Federated), and if so, with what ePPA?
- Have you stated which types of guest transactions need to be logged for auditability (provisioning, updates, de-provisioning, reactivation of accounts, access/authorization, etc.)
- Have you stated whether guest authentication is to be logged/audited differently than member authentication?

Business Practices

Self-Assessment Questions

- Is there a standard business practice for evaluating the eligibility of individuals for guest/affiliate accounts?
- Is there a standard process, with or without an approval workflow, to designate individuals who can sponsor guests?
- Are there standard rules regarding what documentation is to be kept, along with where and for how long, with regard to sponsors? (e.g. sponsor approvals, guests sponsored, etc.)
- Is there a standard process for renewing a sponsor?
- Is there a standard process for replacing a sponsor (e.g. after one retires or severs employment), and does that include what happens to active guests (and their accounts) that were sponsored by the outgoing person?
- Have you decided whether to store guest data in its own data store or with other "member" data? For what reason(s)?
- Will services that consume identity data about guests differentiate between guests and "regular" members (e.g., alert services)?

- Are the appropriate support processes for guests (e.g. initial password distribution, account claiming, password reset, assistance with services) in place and well communicated?
- Is there a standard process for terminating/renewing a guest (credential)?
- Can a guest credential (ever) be reused by someone else?
- Are the appropriate consequences of misuse of a guest credential established and well communicated, especially to the guest, the sponsor, and the department?

Technical

Self-Assessment Questions

- Are any schema extensions to any of your data repositories required for handling guests and sponsors (that will need to be maintained)?
- Are any new/customized forms (paper or online) required for handling guests and sponsors (that need to be maintained)?
- Is there a new/customized identifier generation algorithm required for handling guests and sponsors (that need to be maintained)?
- Are there other systems that required modifications for handling guests, sponsors, and their attributes (e.g. directory, student/employee/guest System(s)-Of-Record or SORs)?
- Are any new/customized attribute values required for assignment to guests and sponsors (that need to be maintained)?
- Are any modifications to your provisioning system/tools required to support guests and sponsors?
- Are any modifications to your de-provisioning system/tools required to support revocation and expiration of guest credentials and sponsor access?
- Are modifications to your authentication system required to support guest credentials?