Key decisions regarding requirements for (or lessons learned from) USF's Affiliate/Guest ("VIP") system, as of January 2011:

1. Reduce the need to put identity-records in the student and employee systems of non-student-related-people and non-employee-like people, e.g. contractors, volunteers, seminar-attendees, summer-campers, vendors, external auditors, trustees.
2. Offer a self-registration capability, so that minimal (virtually "public") services can be automatically provisioned without involving a USF employee.
3. Make it relatively easy for "trusted" USF employees to sponsor their guests (visiting researchers, volunteers, etc.) for services.
    a. Provide a means (at least manually by the IT-Security office) to provision and de-provision "trusted sponsor" status to employees. So far only a few dozen appear necessary, but we must allow for this to increase as more people become aware of the new process and stop using undesirable methods for getting their guests into USF systems.
    b. Allow the same employee to sponsor multiple "guests/VIPs", but only allow the same "guest/VIP" to be sponsored (at least as a "primary" sponsor) by one employee at a time.
    c. Also make it relatively each for "trusted" USF employees to manage their sponsored guests, including ending their relationship earlier than planned, or extending it beyond originally planned.
4. Allow "guests/VIPs" to be easily provisioned at least temporary network-IDs (typically for access to our labs or wireless networks) and/or ID-Cards.
5. Use a single identifier in the provisioning system for both "guests/VIPs" and identities from our (student and employee) systems-of-record.
6. Since we want to store more attributes (and history) than are directly relevant to our provisioning system, use a place outside of (at least the "normal" portion of) the provisioning system to store "system of record" information that can vary over time about "guests/VIPs" (e.g. someone sponsored by the Math department one year might come back the following year sponsored by the Physics one).
    a. Since our provisioning system is "homemade", we could do this by adding a few extra tables and web pages.
7. Separate the "guest" population into 2 main groups, especially for determining eligibility for services and retention:
    a. Self-registered ones, which we have little trust in their identity, since it's self-reported with minimal verification – So far these are only eligible (even if they provide "sufficient identifiers") for disposable NetIDs and disposable ID-Cards.
    b. Sponsored ones, which we have more confidence in their identity, since a USF employee is held responsible – These are eligible for services based on their affiliation, just like people from the student and employee systems-of-record.
8. Require at least the following minimal pieces of identity information for self-registered "VIPs", but also allow collection of other pieces (e.g. phone):
    a. First-name
    b. Last-name

   c. Date-of-birth
   d. Email-address (obviously external)
   e. Phone (within USA only)

9. Require at least the following minimal pieces of identity information for sponsored “VIPs”, but also allow collection of other pieces (e.g. planned location on campus):
   a. First-name
   b. Last-name
   c. Date-of-birth
   d. Email-address (obviously external)
   e. Phone (within USA only)
   f. ID of Sponsor (validated, and used to map to phone, email, etc.)
   g. Planned end-date
   h. Cohort
10. Apply the same “sufficient identifiers” restriction (which we have as our “silver rule” – you must have a first-name, last-name, and date-of-birth or SSN) to sponsored “VIPs” before allowing them to “feed” elsewhere.
    a. For example, people who don’t meet our “silver rule” are kept out of our central person-registry and do not receive an official USFID (e.g. U12345678). At best they can receive a temporary Affiliate-ID (e.g. A12345678), which is treated differently by our service-providers.
11. For self-registered “VIPs”, create a temporary USF NetID (e.g. ‘usf001’) during the web registration process, and deliver the activation code via email or phone. Create ID-Card upon demand (at the ID-Card office, not online).
    a. Do not allow password resets on temporary NetIDs.
    b. Purge temporary USF NetIDs after a set period of time, e.g. 3 months.
12. Ensure that provisioned-services are appropriately terminated (for “guests/VIPs” too) upon the end-date of the corresponding sponsorship/affiliation. Note that ID-Cards cannot be “terminated”, but their status can be set to “inactive”.
13. Also ensure “guests/VIPs” are included in periodic audits of (active) provisioned-services versus current university roles/affiliations.