Vetting, Proofing and Registration Focus Group

Group Participants

Masume Assaf, University Office of International Programs
Jason Gilham, University Outreach
Paula Hamaty, University Outreach
Tom Irwin, Commonwealth Campus
Cindy Kellerman, Houseing and Food Services, ID+ Office
Steve Kellogg, Information Technology Services, Applied Information Technologies
Linda Klimczyk, University Libraries
Jerry Mihally, Information Technology Services, Digital Credential Services
Steve Selfe, Office of Human Resources
Jim Smith, Office Physical Plant
Neal Vines, College of Ag Sciences

Overview:

As a sub-group of the Identity and Access Management (IAM) Committee, the Vetting, Proofing and Registration Authority Focus Group was charged with identifying the elements of the processes needed to facilitate the proper registration, vetting and digital credentialing (VPC) of our constituency for the purpose of properly supporting computer-based applications. To that end of identifying the elements of the processes involved, a continuum of elements was identified. The table representing this continuum is presented in the Appendix. This is, by no means, an all-inclusive list of the possible actions or elements of a set of processes for end-user credentialing. In so creating this continuum, we did get to the point where we felt that we were going beyond what we believed was our charter of developing a common language and roadmap for the future of IAM at Penn State. For posterity and future consideration, we include here what was discussed during the meetings.

In identifying the overall process and elements of VPC, it was necessary to develop a set of working definitions and a set of recommendations to facilitate institutional identity and access management.

Definitions

Overall Process:
The complete set of processes used to manage, create and support the assertion of one’s digital identity. This encompasses the data collection, data validation, proofing, and credentialing with regards to various authentication mechanisms. Re-vetting, re-proofing and re-credentialing have a place is the overall process for digital identity and access management. (See Appendix A)
**Affiliate:**
A person who has an identified, official standing with the university. One who is attached to the university in some way.

**Vetting:**
The process by which data is acquired on an affiliate and, to the extent possible, the data is validated and/or verified for authenticity.

**Re-vetting:**
The process of re-acquiring and/or acquiring new data for an affiliate and/or validating and/or revalidating the new or previously acquired data for that affiliate.

**Proofing:**
The act of aligning someone’s previously recorded data to the actual person, most notably at the time of issuance of credentials.

**Re-proofing:** The act of proofing again.

**Credentialing:**
The act of issuing the token that will be used to establish the digital identity of someone.

**Re-credentialing:**
The act of reissuing a token to a previously credentialed individual. A password reset is an example of re-credentialing. A password change by the end-user is not.

**Registration Authority:**
The organization or individual that applies and executes the policies and procedures established by the institution to affect the collection and validation of end-user data and the issuance of credentials and/or authentication tokens to end-users.

**Root Registration Authority (RootRA):**
The identified Penn State organization that owns the overall responsibility for the vetting, proofing and credentialing of end-users. The RootRA also owns the responsibility for vetting, certifying and auditing of Delegated RAs. The RootRA will have the overall Authorization to Operate the Digital Identity Management System.

**Delegated Registration Authority (DRA):**
Individuals appropriately authorized by the root RA to perform the duties of the RA to collect and validate information and issue credentials. A delegated RA can only issue credentials to an LOA that they are authorized.

**Person Registry:**
A single, authoritative system of record that defines all affiliates of the university/enterprise, and also serves as a data store of all of the information that is held to define the digital profile of the affiliate.
Recommendations

1. Streamline Vetting, Proofing and Credentialing Processes:
In order to improve the effectiveness and timeliness and to mitigate frustration when credentialing and re-credentialing end-users, we should streamline our processes for vetting, proofing and credential issuance, along with provisioning.

- **Rapid Issuance of Digital Credentials:** With the ever-increasing need for one’s digital credentials before being able to do many things at Penn State, much faster credentialing needs to be accomplished. Consideration should be given to establishing, within reason, goals for rapid credential issuances. The group discussed 2 hours as being a reasonable goal for the issuance of a credential.

- **Person Registry Information:** In order to facilitate more timely digital credentialing, real-time updates of relevant information should be a goal. Employing principles of Service Oriented Architectures (SOA) makes sense for helping to attain this goal. A central Person Registry maintained with real-time or near real-time updates is an example of a component in expediting the process.

- **Review Signature Stations:** The current signature station process takes too much time to complete, has weaknesses that allow for circumvention of the intended purpose of proofing an individual, and does not employ adequate technology for capturing a good facsimile of an end-user’s signature. The role of signature stations should be reviewed
  - To remove non-essential elements that have been added to signature station processing
  - To determine if the most current technology is being used
  - To insure process compliance
  - To improve by making more efficient and simplifying the current process
  - To determine if end-user signatures are still necessary

- **Leverage existing proofing activities:** Another opportunity for streamlining and significantly improving the process for proofing and credential issuance is to have an appropriately authorized person who conducts good person proofing now for other purposes be able to easily issue the digital credential at the same time. Otherwise, it is a missed opportunity to capitalize on that moment of (good) proofing. This will also keep the end-user from having to do it again for the sole purpose of obtaining the digital credential.

- **Self-service Re-credentialing:** It is felt that the lack of a reliable method for self-service password resets creates an undue burden on our constituency and, also, promotes an inconsistent application of procedures for password resets around the university. The recommendation is to provide such a self-service password reset
mechanism. It is recognized that utilizing such a mechanism might lower one’s LOA.

- **One authentication domain:** To help eliminate the confusion generated by FPS and Access Accounts, merge the two authentication domains into one and better utilize appropriate authorization for access to all applications once the identity of an individual is established by whatever means available.

2. **Protect and Secure Penn State Digital Credentials:**
To insure the integrity and security of the Penn State Authentication domain, consideration should be given addressing a number of issues that we believe potentially compromise the domain.

- **Authentication Name Space:** Establish a policy that places restrictions on the use of Access Account userids by external (out-sourced) service providers such that they can only authenticate via the PSU password store. It is often the case when departments outsource application services that the decision is made to use a local (to the application) authentication mechanism and use Penn State Access Account userids. It is felt that there is a likelihood that most people will use the same password with that userid as they do for real Access Accounts, thus affectively compromising the security and integrity of the PSU authentication domain. (The foreign entity/company will have the full clear-text credential (userid and password) in their possession.) The policy should stipulate that if the foreign service provider cannot or will not use a secure authentication method that does not expose the password to them, such as our websso or an identity federating technology, then they should be forbidden from using the Penn State Access Account ID/Namespace.

- **Multiple Passwords:** Multiple accounts and passwords inadvertently lead to users writing down this information in potentially accessible places (sticky notes on computer monitors). This creates undue security risks. We should eliminate the use of multiple authentication domains for Penn State applications. In addition to Access Account passwords, one might typically have separate passwords for IBIS/ISIS, Data Warehouse, local applications, etc. We should seek to eliminate this multiple password situation to the extent possible.

- **Domain Authentication Tokens:** All authentication tokens or credentials that pertain to the overall Penn State Identity and Access Management System should fall under the purview of the Root Registration Authority for the proper application of policies and procedures. RSA SecureID tokens and Public Key Infrastructure are examples of authentication tokens that should be administered by the Root RA.

3. **Delegated RAs:**
To insure the integrity and security of the overall digital identity management system, new training, certification, auditing and governance strategies should be considered and employed.

- **Certification of DRAs:** A training and certification program should be developed for Delegated RAs (DRA) to ensure their understanding and sensitivity to the importance of compliance with and for the policies and procedures associated with being an RA. They should get certified only to a level (LOA) that is necessary and only for specific affiliates that is necessary for their respective constituency. There should be real consequences for non-compliance with the established policies and procedures. We propose, at a minimum, the loss of the authorization to operate as a DRA.

- **Automatic management of DRA Role:** It is recommended that a DRA’s authorization to operate be maintained by a central role so that their privilege is quickly revoked if necessary, such as would probably result from a job or position change.

- **DRA Justification:** We should develop specific criteria along with a process for the justification of having a DRA in or for a given area of the university.

- **Review current DRAs:** All people with authorization to perform RA functions now should be reviewed and, in many cases revoked, as soon as possible to close exposures in policy and procedure administration that we believe to be occurring.

- **Limit number of DRAs:** A closely maintained limit on the number of people with RA privileges should be considered.
Appendix A: Basic VPC Process

(Vetting)

Data Collection → Data Validation (or not) → In-person Proofing (or not) → Credential Issuance → Digital Identity Established

Re-Vetting → Re-Proofing

Appendix B: VPC Continuum

<table>
<thead>
<tr>
<th>Vetting</th>
<th>Proofing</th>
<th>Credential Issuance</th>
<th>Password Reset/Re-credentialling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Acquisition</td>
<td>Data Validation</td>
<td>Local</td>
<td>Self-service - immediate issuance</td>
</tr>
<tr>
<td>Name</td>
<td>Birth Certificate</td>
<td>In person</td>
<td>Issued via USMAIL by Delegated RA after non-in-person vetting and proofing</td>
</tr>
<tr>
<td>Address</td>
<td>Test Scores</td>
<td>Driver’s License</td>
<td>Via phone after sufficient verbal proofing</td>
</tr>
<tr>
<td>Email</td>
<td>Email Response</td>
<td>Military ID</td>
<td>Via phone after sufficient proofing -</td>
</tr>
<tr>
<td>Source</td>
<td>Method</td>
<td>ID</td>
<td>Security Measures</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Phone</td>
<td>Call Back</td>
<td>Passport</td>
<td>After phone proofing, USMail token - forced password reset</td>
</tr>
<tr>
<td>SSN</td>
<td>SSN Card</td>
<td>Forced password reset at the time of in-person proofing (current practice)</td>
<td></td>
</tr>
<tr>
<td>Driver’s License #</td>
<td>US Driver’s License</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place of Birth</td>
<td>I9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passport #</td>
<td>US Visa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Military ID</td>
<td>Foreign Driver’s License</td>
<td></td>
<td></td>
</tr>
<tr>
<td>School ID</td>
<td><strong>Distance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Faxed ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Q/A of personal info -“Challenge-Response” Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>US Visa</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3rd Party In-Person</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Proofing (Notary/Other trusted person)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>