Overview

Level of Assurance (LoA) is a term used to describe the degree of certainty that an individual is who they say they are at the time they present a digital credential. The level of assurance group is recommending five levels of assurance to support access to current and future business processes, applications, and data. Our recommendation is to closely align the requirements for levels of assurance at Penn State with the National Institute of Standards and Technology (NIST) document 800-63 and the federal government’s Office of Management and Budget’s M04-04 while addressing the needs of the university. This alignment will allow us to support federating of identities with peer institutions, business partners, and the federal government.

For the purpose of this document, the degrees of certainty, or LoA’s, will be defined as 0 through 4 with 0 being the lowest degree of certainty and 4 representing the highest. There are a number of factors affecting the degree of certainty related to an individual’s digital identity. The assertion of the digital credential will take place as the individual requests access to a specific service, and vetting, proofing, authentication type, protocols, and credentialing/re-credentialing should all be factored in when determining the level of assurance of the digital credentials.

Registration Authorities (RA), both the root and authorized delegates, will be assigned a maximum level of assurance they are able to assign to an individual’s digital identity. The level each RA is eligible to issue at will be determined by an advisory group based on the recommendations of the IAM - Vetting, Proofing, and Registration Authorities Group.

Vetting

Vetting consists of the acquisition of data and the validation of that data. This process will be done on a continuum starting with level 0 and building on each level with the addition of data acquired along with the origin of the data and type of validation. Level 0 of assurance will require data provided by the user with minimal validation. It is recommended that an email address be provided and validated. Level 1 will accept user provided data with some third party validation. An example of third party validation for a student is the submission of a high school transcript which validates the information entered by the student. Level 2 of assurance will require the data validated at both levels 0 and 1 along with additional data elements. The amount of information collected and validated should continue to rise as the level of assurance increases. An example of data required for levels of assurance 0 through 4 can be found in Appendix A.

Proofing

In person proofing will be required for levels of assurance 2, 3, and 4. In person proofing can be done by the university registration authorities or a trusted 3rd party authorized authority such as a notary. Proof of identity is based on
possession of a valid current primary Government Picture ID that contains applicant’s picture, and either an address or nationality (e.g. driver’s license or passport).

**Authentication Type**

The minimal recommendation is a userid/password pair for access to resources requiring a level of assurance 0, 1, and 2. The password strength should increase as the level of assurance rises with password policies for each level. Level of assurance 3 will require a second factor of authentication. This second factor will need to comply with the federal government guidelines. Penn State currently uses the RSA SecurID token for a second factor of authentication. This technology is one of the few recommended by NIST. There will likely be services and applications that will require a second factor of authentication for affiliations beyond the current faculty and staff that have second factor. The distribution and activation of second factor authentication tokens should be done by registration authorities that meet the requirements to credential at a level 3.

**Authentication Protocols**

The protocol and methods used to distribute and activate Access Accounts and additional factors of authentication should adhere to the recommendations of NIST. Also, the protocols used during the authentication process need to adhere to the same guidelines. Plain text passwords should never be sent and if they are, the certainty of the individual is very low. At all levels of assurance, cryptographic operations are required between the individual and the identity provider: Cryptographic operations should be done in compliance with NIST recommendations.

**Credentialing (Re-credentialing)**

Levels of assurance will be determined based on the processes used to issue and reissue credentials. The processes for both issuing and reissuing will be the same. If an individual loses his or her password and is a level 2, the individual will need to go through the same processes, such as in person proofing, to reestablish their identity. A recommendation is being made by the Vetting, Proofing, and Registration Authority
## Appendix A

<table>
<thead>
<tr>
<th>LoA</th>
<th>Data Collected</th>
<th>Vetting</th>
<th>Proofing</th>
<th>AuthN</th>
<th>Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 4</td>
<td>Data from LoA 0 thru 3 and more</td>
<td>3rd Party with security clearance</td>
<td>*In Person + Security Clearance</td>
<td>Public/Private Key pair and key store password</td>
<td>Hershey Medical Center Applied Research Lab</td>
</tr>
<tr>
<td>Level 3</td>
<td>Data from LoA 1 &amp; 2 and more from both user and 3rd party</td>
<td>3rd Party validation</td>
<td>*In Person</td>
<td>Two Factors</td>
<td>Workflow Role Assignment</td>
</tr>
<tr>
<td>Level 2</td>
<td>Name, DOB, Contact Information</td>
<td>3rd Party validation</td>
<td>*In Person</td>
<td>Userid Password</td>
<td>Signing promissory notes</td>
</tr>
<tr>
<td>Level 1</td>
<td>User provided email address and phone number</td>
<td>Email or callback</td>
<td>None</td>
<td>Userid Password</td>
<td>Email, calendar</td>
</tr>
<tr>
<td>Level 0</td>
<td>Optional, user provided</td>
<td>None</td>
<td>None</td>
<td>Userid Password</td>
<td>Purchasing Ice Cream, paying tuition</td>
</tr>
</tbody>
</table>

*Note: The matrix above is intended to provide visual representation of what levels of assurance at Penn State might consist of how they might be differentiated. This is not an inclusive list of all data elements collected or vetted.*