Charter and Scoping

Charter

Determine if there are alternative ways to deploy AD to ensure compliance with InCommon Bronze and Silver. If there are, develop an Alternate Means Proposal for the set of practices identified (which may be some form of the Cookbook) and submit to InCommon for review. If the risks addressed by the profiles cannot be mitigated adequately using AD, develop community and specification recommendations for next steps.

Scoping

There are two primary dimensions to selecting a scope for this effort:

- Deciding which Active Directory products to include
- Deciding which IAP v1.2 requirements to include

Active Directory Products

The most pressing use cases for many campuses are related to their dependence on Active Directory - Domain Services (AD-DS) in various ways within their IdMS. Based on this, the following use cases have been prioritized:

- Windows 2008R2 AD-DS used as the verifier for the IdP
- Windows 2008R2 AD-DS storing a provisioned copy of the credentials but not acting as the IdP's verifier

For each of these cases, AD-DS may be an on-premise deployment or be hosted by a service provider.

IAP Requirements

A review of IAP v1.2 indicated the following requirements should be in scope because they apply to the use cases listed above and AD-DS may have special challenges meeting the requirements:

- 4.2.3.4 - Stored authentication secrets (S). Challenges related to use of Approved Algorithms.
- 4.2.3.5 - Basic protection of authentication secrets (B).
- 4.2.3.6 - Strong protection of authentications secrets (S). Challenges related to use of Protected Channel.
- 4.2.5.1 - Resist replay attack (B, S).
- 4.2.5.2 - Resist eavesdropper attack (B, S).
- 4.2.8.2.1 - Network Security (S). Challenges related to use of Protected Channel.