Potential Agenda Item for UCTrust meeting

From:	Eric Goodman <ericg@ucsc.edu>
To:	David Walker <David.Walker@ucop.edu>
Subject:	Potential Agenda Item for UCTrust meeting
Date:	Mon, 24 Mar 2008 14:29:24 -0700

Hi David,

Sorry for all the last minute-ness... been somewhat swamped with our first "SIR" cycle since our new IDM system went live.

Something we've been looking at (and I've raised at UC Trust meetings before) is what criteria we will use locally at UCSC to determine when it is (or is not) okay to include new applications in our Authentication service. As we've discussed in the past, there's two aspects to this:

(1) What level of security is UC Trust intending to offer? E.g., is the UC Trust authentication service intended to be sufficient for access to systems with HIPAA data? Are there applications to which we would say "we're not good enough for your authentication needs"?

(2) What (if any) additional risk of breach is encumbered by each participating application by the addition of a new application into the SSO mix? E.g., adding an application whose users are known to share passwords would probably undermine the security of other UC Trust applications that strongly expect their users to maintain confidentiality of their passwords.

So with all that as background, do we have guiding principles that tell us what "sorts" of applications should be considered appropriate for UC Trust inclusion and what shouldn't? E.g., a coworker told me this AM that TAS is interested in exploring using UC Trust to authenticate students. Is that an appropriate use of UC Trust? How would we/they make that determination?

I'm not so much interested just because of UC Trust, it's more that this (how to determine what "can and can't play") is still an issue that is slowing UCSC in deciding how to move forward with UC Trust, Shib and other SSO ventures here at UCSC. So I'm looking for frameworks I can steal.

--- Eric