Subject: Letter to FSA
From: Jim Farmer <jxf@immagic.com>
Date: Fri, 14 Aug 2009 16:29:52 -0400
To: Tim Cameron <tcameron7185@bellsouth.net>
CC: Tim Bornholtz <tim@bornholtz.com>, Randy Timmons <rtimmons@sigmasys.com>

Enclosed is a copy of my letter to Federal Student Aid, U.S. Department of Education. This is a public document and can be retrieved from http://www.immagic.com/eLibrary/ARCHIVES/GENERAL/IMM/I090813F.pdf. It also includes a copy of the transmittal email with some additional context.

There are two issues:

The most serious is possible unintended non-compliance with FERPA. I believe this would apply only to communications between students and financial aid data at the college or university or servicer (including SSL exchanges). Traditionally the Department has been tolerant of transitional non-compliance. However if a student or his parents were to initiate litigation, the Department's tolerance would have little effect in court (speaking as an expert witness with hundreds of yours in the courtroom). I don't expect an immediate response from FSA and possibly no response at all. If we were able to have a meeting with FSA, which could never be scheduled, it is unlikely I would have made my interpretation public. And, of course, I could be wrong in my interpretation. However, in a 2006-2007 study by the University of Manchester leading to a recommendation to implement NIST Special Publication 800-63 levels of assurance. Professor Zhang wrote:

In terms of user registration, identity vetting and record keeping, 67% of IdPs do not satisfy even minimum record keeping requirements for the NIST level 2. In terms of criteria for password selection, periods of validity and the number of unsuccessful attempts allowed, none of the [university] respondents could satisfy even the minimal requirements for NIST level 1.

Zhang continues:

The questions included in the Identity Project's survey revealed that there was a perceived need for "graded authentication" (i.e. LoA), although there was a lack of confidence in their ability to implement it.

[His report can be retrieved from www.immagic.com/eLibrary/ARCHIVES/GENERAL/JISC_UK/J071105Z.pdf].

Which is the consensus of those participating in the discussions following Charlie Miller's 2003 presentation in Austin, Texas. In the discussion the University of Texas had implemented some levels of assurance. They report it would be very difficult for the registrar to meet Meteor guidelines, which are similar to the NIST specifications for LoA Level 2. NIST 800-63 did not emerge until 2006. [See www.immagic.com/eLibrary/ARCHIVES/GENERAL/PESC/P031022C.pdf for presentation slides from the conference].

In the long run the more difficult issue is the data transport specification. Although PESC does have a recent data transport specification, I don't see it used in forthcoming implementations.

The first is likely to be the RS3G pilot expansion. The pilot was implemented between a university in Poland and one in Italy. This was first revealed in late June at the RS3G Workshop. [Notes are available from www.immagic.com/eLibrary/ARCHIVES/GENERAL/IMM/I090805.pdf]. At the same presentation the list of potential universities was long beginning with all of the universities in Sweden. I have been unable to learn any details of the implementation, but expect to meet with the developers in October.

The second will be the K-12 to colleges and universities, likely multiple servicers with multiple, but similar, specifications unless SIFA is able to get consensus. It appears that 25 state systems will be funded from the stimulus funds under conditions that require immediate implementation.

jim

--
Jim Farmer
im+m +1-202-296-7498 (voice mail available)
cell phone +1-405-408-9264
Georgetown University 202-687-0126 (no voice mail please)

I090813F.pdf	**Content-Type:** application/pdf **Content-Encoding:** base64