Shibboleth Security Advisory - 24 October 2011

From http://shibboleth.internet2.edu/secadv/secadv_20111024.txt:

> *A flaw exists in the algorithms specified by the XML Encryption standard that can lead to exposure of personal information under certain circumstances.*
>
> *There is no simple fix for this issue, so deployers are encouraged to consider their use of certain software features and possibly make changes to their configurations if circumstances warrant, as described below.*

The impact for SWAMID is limited since most SPs already use HTTPS. Those SPs that do not today use HTTPS are strongly encouraged to do so as soon as possible.