

Case Study: University of Maryland, Baltimore County

BACKGROUND

UMBC has taken a centralized approach to authentication, but does not require the use of a consolidated authentication service. Instead, we have leveraged integration with the portal to consolidate our services: People that use our WebISO get to integrate their application into the portal.

We implemented centrally-defined usernames (netids) in the early 90's and deployed Kerberos for authentication. Over time, we have migrated to synchronizing passwords in both Kerberos and our LDAP directory through a web-based password changing application. For Microsoft Active Directory, we use cross-realm authentication to make that work, but some applications, such as logging into a Unix shell, use Kerberos directly. Email followed closely by our portal are the most widely used services on campus.

LEVELS OF ASSURANCE

UMBC is moving to adopt the NIST 800-63 standard for passwords and will require that all passwords for critical services, such as financial, payroll, or student meet the NIST LoA 2 assurance strength. We anticipate achieving this by fall 2006.

To move to NIST LoA 2, we examined our password risks. As a result, we eliminated telnet usage on campus, and, in spring of 2006, started a program to disallow clear-text password usage in email and ftp. All unsecured services will be eliminated in 2006.

Furthermore, we plan to define multiple levels of assurance and support levels 1 through 3 during academic year 2006-2007 and are reviewing different options for the second authentication factor. We have a license for a technology called [Passfaces](#), but our preference is to deploy either a smart card or PKI, which would take more time to deploy but would offer better long-term support for encryption.