Questions for Microsoft

Background

On October 6, 2011, Steven VanRoekel, the Federal Chief Information Officer, issued a memorandum (http://www.howto.gov/sites/default/files/omb-req-externally-issued-cred_0.pdf), specifying a timetable for federal agencies to begin leveraging externally-issued credentials. The Federal Identity, Credential, and Access Management Subcommittee (FICAM - http://www.idmanagement.gov/pages.cfm/page/ICAM) is named as responsible for certifying the entities that may issue such credentials.

InCommon (http://www.incommon.org) is a Trust Framework Provider, certified by FICAM under the Trust Frame Provider Adoption Process (TFPAP - http://www.idmanagement.gov/documents/FICAM_TFS_TFPAP_v1.1.0.pdf) at assurance levels 1 (InCommon Bronze) and 2 (InCommon Silver). As a certified trust framework provider, InCommon is authorized to certify campuses to issue identity assertions over the Internet to government agency service providers at assurance levels 1 and 2. The documents governing InCommon's trust framework are available at http://www.incommon.org/assurance/components.html; of particular relevance here is "Identity Assurance Profiles - Bronze and Silver" (IAP - http://www.incommon.org/docs/assurance/IAP.pdf)

The InCommon Assurance Program is currently sponsoring a group of university representatives who are exploring means that can be used to certify for InCommon Silver when password credentials used for Silver-level authentication are stored in an Active Directory instance. "IAP Requirements and Gaps for Active Directory Domain Services" (https://spaces.at.internet2.edu/x/BA8wAg) is a brief summary of that work.

Finally, universities are (multi-vendor) "BYOD" environments. While standards for end-user devices are often established, typically little enforcement is exercised over the types and configuration of devices that may be used to access services. It is important that services be capable of protecting themselves from non-compliant end-user behavior.

Questions

1. Protected Channels - IAP 4.2.3.6.1b - Gaps
    a. RC4 HMAC encryption is not NIST or FIPS approved, and we would like to determine if it's comparable to those methodologies that are. Can you help with this? (See http://www.incommon.org/assurance/alternativemeans.html for the criteria we will consider.)
    b. Currently, it is not very practical to crack RC4 HMAC, even though it has long-known vulnerabilities. If that were to change (*e.g.*, a simple crack program posted on the Internet), does Microsoft have a response procedure for such compromises? How will this procedure protect Microsoft's customers that may be operating at LoA-2 via an alternate means exception?
    c. What encryption algorithms does Windows Secure Channel use?
    d. What's the impact of turning on the FIPS setting on all Domain Clients? What's the impact on Domain Controllers?
    e. As NIST has observed, the initial key used by Kerberos is typically encrypted only by the user's password, which enables brute force attacks against the password. Does AD have mitigation for this? Does NTLMv2 also have this vulnerability?
        i. For reference to this issue see NIST 800-63-1, the following sections:
            1. Section 3: The definition of Kerberos on page 10, calling out known vulnerabilities against offline attacks
            2. Section 8.2.2, Footnote #26, which defines criteria for "impractical" eavesdropping attacks
            3. Section 9.3.2.2, describing that "...the use of Kerberos keys derived from user generated passwords is not permitted at Level 2 or above."
2. What should one do to enable distinguishing between NTLM v1 and v2 in the logs? We would like to downgrade a user's assurance level if they access a service that employs NTLM v1. To generalize, we're looking to detect the overall technical context of the authentication event: protocol, encryption algorithm, tunnel, client platform options, *etc*. Is this information available?
3. When BitLocker full disk encryption is used are disk sectors decrypted only as they are read? What is the recommended/supported BitLocker configuration for use with AD-DS?
4. Does Syskey use NIST/FIPS Approved Algorithms for encryption?
5. Are AD-DS password credentials replicated and stored by other Microsoft identity management components, such as ADFS or Azure services? If so, what are those components?
6. Does Microsoft have a strategy for supporting compliance with the Federal Identity, Credential, and Access Management (FICAM) requirements at LoA-2, perhaps through Microsoft's partnership with the Kantara Initiative? If so, what is the time frame?
7. Does Microsoft have a strategy for AD integration of non-Windows and old-Windows client platforms that will use NIST/FIPS approved algorithms for transport of passwords over a network? If so, what is the time frame?
8. Is it possible to configure AD so that the NetUserChangePassword and NetUserSetInfo protocols require NIST approved algorithms for encrypting the session over which the password data is passed?
9. Reviewing "IAP Requirements and Gaps for Active Directory Domain Services" overall, are there other issues we should address?