

Mehta Ketan

From: Dallas Bishoff [dbishoff@authsec.com]
Sent: Thursday, December 23, 2004 2:16 PM
To: DraftFIPS201@nist.gov
Subject: Comments on Public Draft FIPS 201

Our company, authsec, serves under contract to the Federal Identity Credentialing Committee (FICC) Shared Service Provider (SSP) Subcommittee as subject matter experts and for other support functions. Our company would like to point out that FIPS 201 requires the use of OCSP, which is in contrast to the Common Certificate Policy established by the FICC for the new federal root. Further the recent release of OMB Memorandum 05-05 requires federal agencies to move towards the use of the Shared Service Providers.

We believe that FIPS 201 should identified that agencies are required to architect their solutions in a manner that will support OCSP, but not make OCSP mandatory. The implementation of OCSP at federal agencies where we provide contract support services would raise their costs significantly through licensing costs, deployment costs of OCSP clients, implementation of OCSP transponders, and related activities. At the agencies that we advise, they do not have a business case to implement OCSP at this time, but we have been careful to help them protect for a future OCSP requirement should one present itself.

Again, the mandatory provisions of OCSP in the FIPS 201 are in conflict with the Common Certificate Policy for the federal root, where OCSP is an optional method of performing certificate validation.

Regards!!!

Dallas N. Bishoff – CISSP, CISA, CISM
Senior Vice President
authsec