Public Comments on CMAC

This document contains the public comments on NIST's March, 2005 draft of SP 800-38B, specifying the CMAC mode for authentication.

I wanted to say that I strongly support Draft 800-38B specifying the CMAC mode of authentication. In particular, I applaud the choice of OMAC1 for standardization as a message authentication code. I have been looking forward to the day where we have standardized on a strong message authentication code algorithm, and so it is a pleasure to see this draft appear. I am convinced this standard will serve us well. Thank you for all your work on this; it is appreciated.

-- David Wagner

Cmt #	Organi-zation	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
1	SSA	Gerry Barsczewski (410) 966-3334	G	Section 5.2 Block Cypher, Page 5	In addition to providing the specifications for the CMAC algorithm, we wish that NIST would discuss the following two specific issues in the document: · The effectiveness and efficiency comparison of the CMAC algorithm versus the hash function-based MAC (HMAC) as described in the FIPS Pub.198; and · The key factors need to be considered by an organization prior to selecting these two different approaches.	
2	SSA	Gerry Barsczewski (410) 966-3334	G	Item 2 Authority, Page 1	It is not constructive to include the following disclaimer in the document: “Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or suspending the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official” NIST is most familiar with all the current federal security standards and guidelines. To avoid any potential misinterpretations by federal agencies, we believe that NIST should assume the responsibility in determining the current mandatory standards or guidelines that the CMAC may contradict. Furthermore, we wish that NIST would resolve all these identified conflicts prior to the release of this document.	