

Internet Draft  
[draft-hoffman-ipsec-aes-prf-00.txt](#)  
June 16, 2003  
Expires in six months

Paul Hoffman  
VPN Consortium

## The AES-XCBC-PRF-128 algorithm for IKE

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

Some implementations of IPsec may want to use a pseudo-random function derived from AES. This document describes such an algorithm, called AES-XCBC-PRF-128.

### 1. Introduction

[AES-XCBC-MAC] describes a method to use AES (the Advanced Encryption Standard) as a message authentication code (MAC) whose output is 96 bits long. While 96 bits is generally considered sufficient for a MAC, it is too short to be useful as a long-lived pseudo-random (PRF) in either IKE version 1 or version 2. Both versions of IKE use the PRF to create keys in a fashion that is dependent on the length of the output of the PRF. Using a PRF that has 96 bits of output creates keys that are easier to attack with brute force than a PRF that uses 128 bits of output.

Fortunately, there is a very simple method to use much of [[AES-XCBC-MAC](#)] as a PRF whose output is 128 bits: omit the step that truncates the 128-bit value to 96 bits.

### 2. The AES-XCBC-PRF-128 algorithm

The AES-XCBC-PRF-128 algorithm is identical to [[AES-XCBC-MAC](#)] except that the truncation step in section 4.3 of [[AES-XCBC-MAC](#)] is \*not\* performed. That is, there is no processing after section 4.2 of [[AES-XCBC-MAC](#)]. Of course, the test vectors in [section 4.6](#) can be used,

but only those listed as "AES-XCBC-MAC", not "AES-XCBC-MAC-96".

### **3. Security considerations**

The security considerations are the same as those in [[AES-XCBC-MAC](#)].

### **4. References**

#### **4.1 Normative references**

[AES-XCBC-MAC] "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", [draft-ietf-ipsec-ciph-aes-xcbc-mac](#). This document is currently in the RFC Editor's queue for publication.

### **5. Author's address**

Paul Hoffman  
VPN Consortium  
**127 Segre Place**  
Santa Cruz, CA 95060 USA  
paul.hoffman@vpnc.org