

AES Ciphersuites for DIGEST-MD5 SASL mechanism

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

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. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate 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/lid-abstracts.txt>

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

Directories on ds.internic.net, nic.nordu.net, ftp.isi.edu, or munnari.oz.au.

A revised version of this draft document will be submitted to the RFC editor as a Proposed Standard for the Internet Community. Discussion and suggestions for improvement are requested. Distribution of this draft is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

This document describes the use of the AES Cipher Algorithm in Cipher Block Chaining Mode, as a confidentiality algorithm for DIGEST-MD5 SASL mechanism.

Table of Contents

<TBD>

1 Introduction

At present, the symmetric ciphers supported by DIGEST-MD5 are RC4, DES and triple DES. The SASL mechanism would be enhanced by the addition of AES [[AES](#)] ciphersuites, for the following reasons:

1. RC4 is a subject to intellectual property claims. RSA Security Inc has claims that the RC4 algorithm is a trade secret.
2. DES is not considered secure.
3. The AES is computationally and memory efficient and has withstood extensive cryptanalytic analysis. It is easy implementable on a variety of software and hardware, including smart cards and handheld computers. The AES is therefore a desirable choice.

This document proposes a new DIGEST-MD5 ciphersuite, with the aim of overcoming these problems.

2 Conventions and Notation

This document uses conventions established by [[DIGEST](#)].

3 Definition of AES ciphers for Confidentiality Protection

This document extends the ABNF definition of cipher-value defined in section 2.1.1 of [[DIGEST](#)].

cipher-value |= "aes"

where

aes

the Advanced Encryption Standard (AES) cipher [[AES](#)] in cipher block chaining (CBC) mode with a 128 bit key. This mode requires an Initialization Vector (IV) that is the same size as the block size.

Section 2.4 of [[DIGEST](#)] defines the value of "n" that is used to construct Kcc and Kcs. For cipher "aes" n is 16. The key for the "aes" cipher is all 16 bytes of Kcc or Kcs.

The IV for the "aes" cipher in CBC mode for messages going from client to server (IVc) consists of 16 bytes calculated as follows:

IVc = MD5({Kcc, "aes-128"})

The IV for the "aes" cipher in CBC mode for messages going from server to client (IVs) consists of 16 bytes calculated as follows:

IVs = MD5({Kcs, "aes-128"})

The IV is XOR'd with the first plaintext block before it is encrypted. Then for successive blocks, the previous ciphertext block is XOR'd with the current plaintext, before it is encrypted.

4 Security Considerations

It is not believed that the new ciphersuite is ever less secure than the corresponding older ones. The AES is believed to be secure, and it has withstood extensive cryptanalytic attack.

The use of MD5 hash in DIGEST-MD5 limits the length of AES key to 128 bit, because a key is the output of MD5 hash (i.e. it can't be longer than 128 bit).

5 References

[RFC 2222] Myers, J., "Simple Authentication and Security Layer (SASL)", [RFC 2222](#), October 1997.

[DIGEST] Leach, P., Newman, C., "Using Digest Authentication as a SASL Mechanism", [RFC 2831](#), May 2000.

[AES] Daemen, J., Rijmen, V., "The Rijndael Block Cipher", <http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf>, 3rd September 1999.

[RFC 1321] Rivest, R., "The MD5 Message-Digest Algorithm", [RFC 1321](#), April 1992.

6 Acknowledgements

This document borrows some text from [draft-ietf-ipsec-ciph-aes-cbc-03.txt](#) and [draft-ietf-tls-ciphersuite-06.txt](#).

7 Authors' Addresses

Alexey Melnikov
mailto:mel@messagingdirect.com

ACI WorldWide/MessagingDirect
900 10117 - Jasper Ave.
Edmonton, Alberta, T5J 1W8, CANADA

[8](#) Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.